TELEFI
project

Summary Report

of the project “Towards the European Level Exchange of Facial Images”

Version 1.0
January, 2021

The project 821284 — TELEFI — ISFP-2017-AG-FORENSIC was funded by the European Union’s Internal Security Fund — Police.

Disclaimers

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The content of this report is based on the information collected within the study of the project “Towards the European Level Exchange of Facial Images”. Should any mistake be found, please let us know at info@telefi-project.eu.

Table of contents

Abbreviations and definitions

1:N – One-to-many database search, also referred to as one-to-many comparison or facial recognition or closed-set identification.

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.

ABIS – Automated Biometric Identification System.

ACE-V – Acronym for Analysis, Comparison, Evaluation - Verification. A scientific method utilized in most comparative processes.[1]

AFIS – Automated Fingerprint Identification System.

Biographic data – Non-biometric personal information about an individual, for example name, date of birth etc.

Biometric data – Digital information about a person's physical or behavioural characteristics used to distinguish him or her from other people. For example, digital information of the face, fingerprints etc.

Biometric match – A determination that two biometric samples (see biometrics below) correspond to the same source based on some level of computer-evaluated similarity. This does not inherently imply that the probe and candidate are the same person.[1] In facial recognition investigative reports, the terms "biometric match" and "match" are usually avoided and the terms "potential candidate" or "likely candidate" are used.

Biometrics – The measurement and analysis of unique physical or behavioral characteristics, especially as means of verifying a personal identity (Webster).[1]

BMP – Image file format that stands for BitMaP image file.

Case data – Information about civil, criminal or misdemeanour case, for example type of crime, date of crime, criminal case number etc.

CCTV – Closed-Circuit TeleVision, also known as video surveillance.

Civil database – Set of data obtained during civil proceedings, for example during issuing of passports, ID-cards and driving licences.

Controlled image – An image captured in accordance with facial identification (FI) or facial recognition (FR) standards or guidelines (e.g., a driver's license photo).[1] Also known as reference images.

Criminal database – Set of data obtained during offence proceedings.

DIWG – Digital Imaging Working Group, an expert working group of the European Network of Forensic Science Institutes (ENFSI).

[1] FISWG Glossary Version 2.0 2019.10.25 https://fiswg.org/fiswg_glossary_v2.0_20191025.pdf

Facial recognition – The automated searching of a facial image (probe) against a known collection resulting in a list of candidates ranked by computer-evaluated similarity score. This is commonly referred to as a one-many comparison.[1]

FR – Facial recognition.

ENFSI – European Network of Forensic Science Institutes.

Enrol/enrolment – Term used within this report to designate the process of entering/registering data into a database.

EU – European Union.

FISWG – Facial Identification Scientific Working Group.

GDPR – General Data Protection Regulation.

GIF – Image file format that stands for Graphics Interchange Format.

ICAO – International Civil Aviation Organization.

Intelligence – Term used within this report to designate information gathering and analysis by law enforcement agencies with the purpose of preventing criminal activity and identifiying criminals.

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission.

JFIF – Image file format that stands for JPEG File Interchange Format.

JPEG – Image file format that stands for Joint Photographic Experts Group.

Lights out – An automated conclusion based upon threshold scores with no human involvement.[1]

Live facial recognition – Real-time search of faces caught by a camera against a watchlist of persons of interest.

Match – See definition of biometric match.

Match rate – Frequency of matches from all search results.

Metadata – Set of data about other data, for example the unique identifier for a facial image in a database.

NIST – National Institute of Standards and Technology.

Personal data – Information used to identify a person, for example name, date of birth, facial image etc.

PNG – Image file format that stands for Portable Network Graphics.

PPI – Pixels per inch.

[1] FISWG Glossary Version 2.0 2019.10.25 https://fiswg.org/fiswg_glossary_v2.0_20191025.pdf

Probe – The facial image or template searched against the gallery in an FR system.[1]

Prüm – Convention adopted into EU legislation stipulating the exchange of DNA, fingerprint and vehicle registration data between EU Member States for law enforcement purposes.

SOP/SOPs – Standard operating procedure/Standard operating procedures.

Template – A set of biometric measurement data prepared by an FR system from a facial image.[1]

TIFF – Image file format that stands for Tagged Image File Format.

UK – United Kingdom.

Uncontrolled image – An image not captured in accordance with FI/FR standards or guidelines (e.g., a surveillance image).[1] Also known as trace images.

[1] FISWG Glossary Version 2.0 2019.10.25 https://fiswg.org/fiswg_glossary_v2.0_20191025.pdf

Acknowledgements

The TELEFI project team is sincerely grateful to all individuals and organisations that have supported the TELEFI study and the preparation of this report.

Most importantly, we want to thank the Internal Security Fund – Police of the EU Commission for awarding the financial grant and for having faith in the TELEFI project initiative.

Furthermore, we would like to express our gratitude to the numerous representatives from law enforcement, forensic and civil authorities in the 27 EU Member States, the UK, and two international organisations (Europol and Interpol). They have played key roles in the project by participating in the survey, welcoming us on study visits and granting interviews. We hugely appreciate your dedication, time, and valuable inputs into the TELEFI study. The completion of this report would not have been possible without your help and cooperation.

Executive summary

The Prüm Convention, signed in 2005, was adopted into EU law in 2008 to support the fight against cross-border crime. It obliges the EU Member States to allow law enforcement authorities from other Member States to perform searches in their national databases, holding data on DNA, fingerprints and vehicle registration.

The Prüm data exchange has been a success story. However, after more than a decade, Prüm has reached a stage where it is reasonable to assess its achievements, examine the problems encountered, and discuss how the data exchange might evolve further. Amongst the other suggestions being made during the current discussions, is a proposal to adopt new data categories in the Next Generation Prüm. The most likely candidate for a new data category is the face modality. This would be the third biometric modality within Prüm alongside DNA and fingerprints.

When contemplating the future addition of the face modality within Prüm, it is essential to have a clear understanding of the national facial image databases that currently exist across the EU Member States and the use of FR by the law enforcement and forensic authorities. To the best of our knowledge, no previous study has conducted an extensive review of FR use across EU Member States. The EU funded project "Towards the European Level Exchange of Facial Images" (TELEFI project) is intended to cover this gap.

The TELEFI project study has aimed to:

- Determine the current situation regarding the use of FR in criminal investigations across the EU Member States.
- Find out which organisations are involved in facial recognition work in the EU Member States.
- Determine the national databases in the EU Member States that contain facial images.
- Describe the software used in the EU Member States both for databasing and FR purposes.
- Determine the quality standards used.
- Describe the legal framework regulating the use of facial images in the EU Member States.
- Describe the current visions within the relevant organisations in the EU Member States regarding the future for international facial image data exchange.
- Make further recommendations for the harmonization of the field across Europe.

In order to meet the aims of the TELEFI project, information was collected from the 27 EU Member States, the UK, Europol and Interpol. The main two methods for data collection were a web-based survey and face-to-face interviews. The survey was carried out using a short questionnaire to collect preliminary data for the study, while the interviews were performed using a structured questionnaire with 112 questions to gather detailed information.

The TELEFI project study has found that (as of December 2020) FR has been implemented in 11 EU Member States (Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, The Netherlands and Slovenia), in the UK and by Europol and Interpol. 7 EU Member States (Croatia, Cyprus, Czech Republic, Estonia, Romania, Spain and Sweden) have reached the stage of preparing for implementation and expect to start using the technology within one to two years. With 9 EU Member States (Belgium, Bulgaria, Denmark, Ireland, Luxembourg, Malta, Poland, Portugal and Slovakia) no solid plans for implementation were presented.

A typical use case of FR by law enforcement authorities in the EU Member States, the UK, Europol and Interpol is as a retrospective tool used during an investigation, where the uncontrolled facial image (e.g. surveillance image) associated with a criminal event, is examined after the crime has been committed. The facial image of interest is searched (1:N) against a database that contains controlled images of known individuals with an aim to identify the person within the image. The search result is a list of candidates which is reviewed by a human operator and a decision is made on any potential match. In most instances, the FR search results are considered investigative leads and are not used as evidence in court. For court purposes in most Member States, a forensic 1:1 facial image comparison must be conducted leading to the formulation of an expert opinion. No EU Member State has implemented live facial recognition for routine use, but it is routinely used in the UK.

Databases in the EU Member States that are used for FR during criminal investigations:

EU Member State	Year of impl.	Database	No. of images	No. of persons	Person categories
Austria	2020	EDE - Criminal identification database	1.25 M	620 000	criminals
Finland	2020	RETU - registered persons identifying features database and Aliens database			suspects, asylum seekers and aliens
France	2013	TAJ - criminal case history database	6 M	21 M	suspects and victims (i.e. unknown dead bodies, seriously injured and missing persons)
Germany	2008	INPOL - criminal case management system	5.5 M	6.2 M	suspects, convicts, arrestees, missing persons, wanted persons and asylum seekers
Greece	2019	mugshot database	Not specified	377 000	suspects who have been arrested and convicts who have been sentenced to imprisonment
Hungary	2016	Facial Image Registry	30 M	Not specified	civil document applicants
Italy	2017	AFIS	17 M	9 M	convicts, arrested suspects, unidentified persons, immigrants and asylum seekers
Lithuania	2019	HDR - Habitoscopic Data Register	400 000	185 000	suspects, convicts, arrested persons, wanted persons, unidentified dead bodies and unidentified helpless persons

Latvia	2012	BDAS - Biometric Data Processing System (criminal data array)	Not specified	Not specified	detained, suspected, accused and convicted individuals, and unidentified dead bodies
Netherlands	2016	CATCH criminal and CATCH alien	Not specified	8.3 M	suspects, convicts, visa and asylum applicants
Slovenia	2015	the record of photographed persons	Not specified	110 000	suspects, missing persons and unidentified dead bodies

Databases in the EU Member States that are expected to be used for FR during criminal investigations in the near future:

EU Member State	Expected year of FR implementation	Database
Croatia	2021	ABIS and image repository of civil documents
Czech Republic	2021	CBIS - Central Biometric Information System
Romania	2021	NBIS - National Biometric Identification System
Spain	2021	ABIS
Sweden	2021	ABIS
Cyprus	2021–2022	ISIS Faces
Estonia	2022	ABIS

The facial image acquisition process varies significantly between the EU Member States. In most instances, facial images are collected at police premises across the country during a process where photographs of a person are captured in parallel with the collection of fingerprints, biographic data and case data. 5 EU Member States declared that special quality standards are applied during the image capture and/or the entry of the images into the database. The standard named by these Member States was ISO/IEC 19794-5. Additionally, 2 of these Member States named the ICAO standard. Even without a standard, SOPs for image capture and image entry have been developed and employed in most EU Member States using FR technology. Two-thirds of the Member States declared to have a training process in place for personnel performing the named tasks.

In most EU Member States, only frontal facial images can be searched using FR. In 6 out of 11 Member States, where FR has been implemented, the searches are performed by a limited number of persons that are specialized in the facial field (Austria, Germany, Greece, Hungary, The Netherlands and Slovenia). The same practice is followed by Europol and Interpol. By contrast, a wide range of police officers requiring the facial modality for operational purposes, can perform searches in Finland, France, Italy, Latvia and Lithuania. In most EU Member States, there are no written instructions in place for performing FR searches. The only Member State that has a validated and accredited method for this task is Sweden (ISO/IEC 17025). The match rate of FR searches (i.e. reporting of a “potential candidate” or “likely candidate”) varied in different countries between 1% to 8.2%.

The legal landscape related to the use of facial images in criminal investigations, varies significantly between the EU Member States from a country that has a dedicated law for FR (i.e. Hungary) to countries where the use of facial images has been regulated by many laws and implementing acts (i.e. most of the Member States). The legal aspects addressed during the TELEFI project have been summarized in a separate report ´The Legal Analysis for TELEFI project´, which is published on the TELEFI project website (www.telefi-project.eu).

Interviewees from most EU Member States (74%) expressed a clear positive attitude towards the extension of the Prüm system with the addition of the face modality and no interviewee expressed a clear opposition to this matter. Furthermore, most consider the European level harmonization of the FR area to be an important prerequisite for adopting the face modality in the Prüm framework. With reference to the potential architecture of the Next Generation Prüm, interviewees from 12 Member States favoured data exchange using the current decentralized solution, whilst 5 Member States favoured a central solution. Interviewees from 4 EU Member States had no clear preference, and no opinion was expressed by 6 Member States.

Based on the information collected within the study, recommendations are presented for the harmonization of the FR area and for the steps that need to be taken to move further towards the exchange of facial images within the Prüm framework. Three of the most important recommendations supported by the TELEFI project results:

1) To move ahead with the introduction of the face modality within the Prüm data exchange.
2) To develop Europe-wide quality requirements for controlled images in the national databases that would be used for Prüm data exchange.
3) To start the facial image data exchange within the Prüm framework by using the current decentralized architecture. At the same time, continue efforts to identify whether EU Member States consider it possible (legal and data protection aspects) to move towards a future with a centralized data exchange.

The results of the TELEFI project along with recommendations have been described in the ´Summary Report of the project “Towards the European Level Exchange of Facial Images”´, which is published on the TELEFI project website (www.telefi-project.eu).

Introduction

The increasing number of surveillance cameras installed in public places and the wide use of image capturing devices (ranging from mobile phones to professional cameras) means that criminal activities are ever more likely to be recorded. Thus, the broad availability of facial images, creates a huge potential for FR to contribute towards the fight against crime and terrorism on both national and international levels.

Currently, the use of FR in the investigation of crime varies a lot across the EU Member States. As this report shows, while some Member States have not yet started to consider the technology, others are beginning to set up FR infrastructures ready for implementation, whilst yet others have been using the technology for several years or even for well over a decade.

Facial recognition in criminal investigations

A FR system usually includes algorithms for finding the face within an image (face finding), for creating a digitized representation of the face (feature vector/template), for comparing the digitized representations of two face images and for computing a numerical comparison result based on their similarity and dissimilarity (score). If the score computed for a candidate is under a defined threshold, this candidate is excluded. If the score is above the defined threshold the candidate is not excluded.

For criminal investigations, the most common use case is the retrospective one-to-many (1:N) search, where an image of an unknown person is searched against a database of known individuals with the aim to determine the identity of the person. The output of the FR system is usually a list of the best candidates, ranked by the matching score. This process is not fully automatic, but includes a role for human operators (e.g. police officers, facial reviewers, forensic experts). An operator is involved in the face enrolment and candidate list review, which is often crucial, especially when working with images of low quality as may arise from surveillance cameras. Typically, the results serve as an investigative lead and are not intended for use as evidence in court proceedings.

Furthermore, in criminal investigations, it is becoming common to use the FR algorithm to cluster together instances where the same person appears in large collections of image and video material. Historically, this has been done manually and can be very time-consuming.

Law enforcement agencies around Europe also seem to show an increasing interest in the potential use of live facial recognition. In this use case, faces caught by a camera in a public space are matched in real-time against a watchlist of persons of special interest, such as wanted criminals. Some trials (e.g. UK experience) have shown that such implementations are more complex with a need to pay careful attention to the legal framework and the requirement for officers to be close enough to the camera to be able to confront any potential matches.

The performance of FR algorithms has evolved rapidly over the last five to ten years and this is clearly demonstrated by benchmark testing, like that performed by NIST[2] in the USA. With the introduction of the deep learning of artificial neural networks, often referred to as artificial intelligence (AI), the measured performance of FR algorithms has improved 20-fold between 2014 and 2018. The performance of FR algorithms has been exceptionally good for some time when working with good quality facial images taken under controlled conditions. Moreover, the current generation of algorithms perform very well, and often better than humans, when working with low quality images, like those from CCTV cameras. Current challenges for the developers include algorithm performance improvements for people wearing face masks and

[2] Face Recognition Vendor Test (FRVT) Ongoing https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

the avoidance of demographic differences (i.e. bias effects). As reported by the Information Technology and Innovation Foundation (ITIF) in early 2020, a recent study by NIST has demonstrated that the best FR algorithms now have undetectable differences between demographics groups[3].

The face modality, when compared to the more well-established biometric modalities such as fingerprint and DNA, is considered to be a young and non-mature discipline. Although there are international organisations like the ENFSI DIWG[4] and FISWG[5] that are working towards harmonization in this field (best practice manuals and guidelines) there are still great differences around the world, e.g. databases accessed, image quality standards, competency and staff training, SOPs and the reporting of results. Even across EU Member States, that all adhere to the GDPR[6], the usage and national legislations for FR vary greatly. There are actions initiated recently, both by the EU Commission[7] and by civil rights groups[8], which address the question as to whether the use of AI and FR should be further restricted, or even temporarily banned. Nevertheless, undisputedly, there are many examples where the technology has helped law enforcement agencies to solve crimes and identify missing persons or abused children. International reports give examples of both success stories and alarming failures, where FR has been used in criminal investigations[9,10]. While the technology has much potential for combating crime, the implementation and usage of FR in criminal investigations needs careful consideration. Inevitably, any implementation of FR in EU Member States must meet the requirements for lawfulness, necessity and proportionality regarding an individual's interests, rights and freedoms.

Importance of the human operator in the process of facial recognition

In general, humans are very good at recognising the faces of people that are familiar to them[11]. However, in general, when it comes to comparing unfamiliar faces, humans are quite poor[12], although some people are more capable than others. It has been shown that to improve human performance in comparing unfamiliar faces, experience with a large number of face comparisons is not enough. Tests in high-throughput environments, such as border control, have shown that the error rates usually have little or even no relationship to the number of years the person has worked with the task[13]. The research strongly suggests that it requires substantial time and effort in dedicated training programs (covering topics such as the characteristics, typicality and stability of facial features alongside comparative methodology and imaging technology) as well as systematic feedback and mentoring[14]. Furthermore, a verification process, involving one or more additional persons, has been shown to drastically

[3] The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms

[4] ENFSI Digital Imaging Working Group http://enfsi.eu/about-enfsi/structure/working-groups/digital-imaging/

[5] Facial Identification Scientific Working Group https://fiswg.org/index.htm

[6] General Data Protection Regulation https://eur-lex.europa.eu/eli/reg/2016/679/

[7] White Paper on Artificial Intelligence – a European approach to excellence and trust https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-european-approach-excellence-and-trust

[8] Civil society initiative for a ban on biometric mass surveillance practices https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en

[9] Facial Identification Success Stories https://fiswg.org/fiswg_fi_success_stories_2020_07_17.pdf

[10] Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[11] Natu, V., O'Toole, A.J. (2011). The neural processing of familiar and unfamiliar faces: a review and synopsis. Br J Psychol., 102(4):726-47. doi: 10.1111/j.2044-8295.2011.02053.x

[12] Hancock, P.J., Bruce, V., Burton, A.M. (2000). Recognition of unfamiliar faces. Trends Cogn Sci. 2000 Sep;4(9):330-337. doi: 10.1016/s1364-6613(00)01519-9

[13] White, D., Kemp, R. I., Jenkins, R., Matheson, M., & Burton, A. M. (2014). Passport officers' errors in face matching. PLoS ONE, 9(8). https://doi.org/10.1371/journal.pone.0103510

[14] White, D., Towler, A., & Kemp, R. I. (2021). Understanding professional expertise in unfamiliar face matching. In M. Bindemann (Ed.), Forensic Face Matching: Research and practice. Oxford University Press.

diminish the error rates. For forensic experts in manual facial image comparisons, who are likely to receive training over several years, the error rates can rapidly diminish by a fusion of the results from only a few experts. In contrast, with untrained persons, it requires the fusion of the results from many people to reach the same performance as the experts. Interestingly, the fusion of automatic and human-based methods has been shown to be particularly successful when it comes to the comparison of unknown faces[15]. Nevertheless, the research in this area is only just appearing, and the general understanding of how human-machine interaction can best be used in face biometrics must still be considered as underdeveloped.

Prüm and its potential developments

The Prüm Convention was signed by Austria, Belgium, France, Germany, Luxembourg, The Netherlands and Spain in 2005. Three years later, in 2008, it was adopted into EU law through Council Decisions 2008/615/JHA[16] and 2008/616/JHA[17] on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. The Prüm decisions established exchange of DNA data, fingerprint data and vehicle registration data between national databases. According to the Prüm decisions, all EU Member States are obliged to allow law enforcement authorities from other Member States to perform searches in their national databases that hold data on DNA, fingerprints and vehicle registrations.

The establishment of the Prüm network in Europe is considered to be one of the very important achievements of the EU. The number of searches performed in 2019 through the Prüm framework was reported to be more than 2.2 million for DNA, around 400 000 for fingerprints and more than 16 million for vehicle registration data.

Although the Prüm data exchange has been a success story, more than a decade has passed since it was introduced and we have reached the stage where there is a need to assess what has been achieved, to review the shortcomings and to plan for future developments. Discussions on the Next Generation Prüm (prüm.ng) were first triggered by the Council Conclusion "On the implementation of the Prüm Decisions ten years after their adoption" from 5 July 2018 (10550/18)[18]. Following on, several initiatives have been launched with the aim to consider the future visions for Prüm. The EU Commission has mandated a consulting firm (Deloitte) to perform the Next Generation Prüm feasibility study. In addition, five EU expert groups have been established in the following areas: DNA, FR, fingerprints, vehicle registration data and other forms of police cooperation.

Deloitte has summarized their results and conclusions within the "Study on the Feasibility of Improving Information Exchange under the Prüm Decisions". This was published in three documents: Final report[19], Advanced technical report[20] and Cost benefits analysis[21]. One of

[15] J. Phillips, A.N. Yates, Y. Hu, C.A. Hahn, E. Noyes, K. Jackson, J.G. Cavazos, G. Jeckeln, R. Ranjan, S. Sankaranarayanan, J.-C. Chen, C.D. Castillo, R. Chellappa, D. White, and A.J. O'Toole. Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Algorithms. Proceedings of the National Academy of Sciences, DOI:10.1073/pnas.1721355115, May 29, 2018.

[16] Council Decision 2008/615/JHA https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615

[17] Council Decision 2008/616/JHA https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0616

[18] Council Conclusion "On the implementation of the Prüm Decisions ten years after their adoption" from 5 July 2018 (10550/18) https://data.consilium.europa.eu/doc/document/ST-10550-2018-INIT/en/pdf

[19] "Study on the Feasibility of Improving Information Exchange under the Prüm Decisions": Final report https://op.europa.eu/en/publication-detail/-/publication/6c877a2a-9ef7-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-search

[20] "Study on the Feasibility of Improving Information Exchange under the Prüm Decisions": Advanced technical report https://op.europa.eu/en/publication-detail/-/publication/3236e6ae-9efb-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-search

[21] "Study on the Feasibility of Improving Information Exchange under the Prüm Decisions": Cost benefits analysis https://op.europa.eu/en/publication-detail/-/publication/503f1551-9efc-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-search

the proposals made by Deloitte was the adoption of the exchange of facial images in the Next Generation Prüm. The FR EU expert group, comprising of specialists from 10 European countries, reached the same conclusion, recommending that the EU legal and technical prerequisites should be created as quickly as possible.

While both the Deloitte study and the FR expert group were of the same opinion on the inclusion of face modality in the Prüm data exchange, different conclusions were reached regarding the future architecture of Prüm. The Deloitte study recommended a switch from the current mesh topology to a star topology, to ease the scalability of the connections to Prüm. In contrast, the FR expert group concluded that the Prüm FR system should be planned and installed in a decentralized network system and any proposals pointing towards central data storage were strictly rejected.

The TELEFI project

The Deloitte “Study on the Feasibility of Improving Information Exchange under the Prüm Decisions” and the work by the FR EU expert group, have indicated a clear interest from EU Member States in the use of FR and the potential data exchange of this fast-developing biometric modality. However, to the best of our knowledge, no previous study has conducted an extensive review of FR use across Europe. This information is essential to help achieve the interoperable implementation of the face modality for law enforcement and forensic practice. Clearly, there is a need to further develop national facial databases and procedures in order to move forward towards the exchange of facial images within the Prüm framework. Furthermore, the end-users in EU Member States had not been systematically interviewed to help understand their visions and opinions about the different scenarios for the future of Prüm.

The EU funded project “Towards the European Level Exchange of Facial Images“ (TELEFI project) is intended to cover these gaps, looking at how FR is currently being used for the investigation of crime across EU Member States. The study has aimed to review the organisational, technical and legal aspects of FR at the European level. In addition, a consideration has been given to the potential for implementing the exchange of facial images within the Prüm framework, from the viewpoint of the end-user.

The TELEFI project has addressed 8 core questions:

1. What are the current practices and procedures across EU Member States regarding the use of facial images in the investigation of crime?
2. Which national and international law enforcement and forensic organisations are involved in FR work across Europe?
3. What national databases containing facial images currently exist within EU Member States and are there any potential new developments on the horizon?
4. What technical solutions (for database management and FR searches) are currently in use for FR work in the EU Member States?
5. What quality standards (if any) are currently being applied for the capturing and use of facial images in the EU Member States?
6. What legal regulations are in place regarding the use of facial images across the EU Member States?
7. What are the current visions within different EU Member States regarding the future international exchange of facial image data?
8. What steps can be taken for the further harmonization of the FR area across Europe?

The results of the study are described in this report and provide a detailed description of the current status of FR in all EU Member States, in the UK and in two international organisations (Europol and Interpol) along with recommendations on harmonizing the field at the European level and for Prüm exchange of facial images. Unless otherwise stated, this report is based on data that has been collected up to December 2020.

Authors

The TELEFI project has been conducted by representatives from six European authorities (listed in alphabetical order) between 1 January 2019 to 28 February 2021:

- Estonian Forensic Science Institute – Andra Sirgmets, Gunnar Tasa, Ivar Prits, Kertu Kulm, Kristin Kikas, Maris Puust, Richard Gill, Silver Salla and Üllar Lanno;
- Estonian Police and Border Guard Board – Hannes Järvine;
- National Bureau of Investigation, Finland – Anthony Laird and Tapani Reinikainen;
- National Forensic Centre, Swedish Police Authority – Elisabet Leitet and Tobias Erlandsson;
- Netherlands Forensic Institute – Arnout Ruifrok and Didier Meuwly;
- State Forensic Science Bureau of Latvia – Maira Čentoricka and Raimonds Apinis.

Methodology

The selection of methodology for the TELEFI project was based on the need to meet the project objectives in order to study the current status of FR use for criminal investigations across the EU Member States and to identify the visions and opinions of the various Member State stakeholders about the potential for implementing facial image exchange within the Prüm framework. Several methods for data collection and analysis were used in order to gather information from the EU Member States.

Preparation of questionnaires for data collection

For data collection, two questionnaires were prepared:

- Survey questionnaire;
- Interview questionnaire.

The survey questionnaire included a set of 9 questions for any EU Member State where FR is being used in criminal investigations and a set of 6 questions for any EU Member State where FR is not being used. The survey aimed to collect the preliminary information on the topics of the study in order to prepare for subsequent interviews.

The interview questionnaire included 112 questions structured into 6 parts:

- Part A – characterization of databases used currently for facial recognition in relation to criminal investigations;
- Part B – current status of implementation of facial recognition and plans for the future;
- Part C – characterization of existing databases that are not yet used for facial recognition in relation to criminal investigations but soon will be (if such databases exist);
- Part D – characterization of civil databases if the person to be interviewed has some knowledge about such databases;
- Part E – harmonization of facial recognition across EU Member States;
- Part F – facial image data exchange with other EU Member States in relation to criminal investigations.

Depending on the interviewed authority and the implementation status of FR, different sets of questions from parts A to F were addressed during the interview. The aim of the interview was to collect more detailed information on the topics of the study.

Data collection

For most EU Member States, the data collection process involved two steps. First, a web-based survey followed by a face-to-face interview as the second step.

52 individuals representing more than 40 law enforcement and forensic authorities in 26 EU Member States (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and UK[22]) and Interpol were invited to take part in the web-based survey.

Out of the 52 invited individuals, 38 representing 34 authorities participated in the survey between May 2019 and May 2020 (see Appendix 1). In addition, an email survey was carried out for the preliminary data collection from Europol in October 2020.

[22] EU Member State at the time of the survey

The participation rate in the web-based survey for the invited individuals (representing 26 EU Member States, with the UK included in the statistics) was 73%.

The survey was not conducted in 2 EU Member States: Estonia and Sweden. Both countries were active participants in the TELEFI study and, thereby, the survey was not considered necessary because the information was already known to the TELEFI project team.

Overall, the number of interviewed law enforcement authorities (including Europol and Interpol), forensic organisations, and other authorities responsible for various civil databases was 64 (see Appendix 2).

Most of the interviews (in 23 Member States: Austria, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden, and at the Interpol) were carried out face-to-face between September 2019 and February 2020. Additional written answers to the interview questionnaire were also received from some of these countries.

The visits for face-to-face interviews in Cyprus, Luxembourg and Europol were not possible because of the COVID-19 outbreak and the lock-downs across Europe. For these Member States and Europol, the answers to the interview questionnaire were received in written form between May and November 2020.

No answers to the interview questionnaire were received from 2 EU Member States (Belgium and Ireland) and from the UK[23]. Thus, the data presented for these countries are solely based on the information collected from the survey. In the case of the UK, additional open public sources have been used.

The participation rate of the EU Member States (UK included in the statistics) in the interviews was 89%.

Data analysis

The data collected via the surveys and interviews were analysed by categorising and synthesising the information. Based on the initial data analysis, individual country and organisation reports were prepared (see sections ´Country reports´ and ´Organisation reports´). The data in the individual reports were analysed further and are presented in the form of generalised data (see section ´Generalised data´).

Data verification

Prior to the publication of this report, between June 2020 and January 2021, there was an aim to verify all the information in the country and organisation reports. In general, the verification process involved the following steps:

1) The country/organisation report draft was sent to the interviewed authority/authorities for commenting/cross-checking.
2) The comments/corrections from the interviewed authority/authorities were taken into account and the report was updated.
3) The updated country/organisation report was sent for a final approval to the interviewed authority/authorities.

Steps 1) and 2) were repeated multiple times, as necessary.

[23] Former EU Member State from 31 January 2020

Most of country reports and both organisation reports have been crossed-checked and approved by the authority/authorities that provided the data.

In situations where several authorities had provided interviews on the same topic, the country report was considered to be approved when at least one of the interviewed authorities had given approval.

For one specific topic (´National registry of drivers´ in the country report for Portugal) a cross-check has been performed, but the final approval has not been received from the relevant authority by 31 January 2021.

A few specific topics have not received any feedback by 31 January 2021 from the authority/authorities that provided the data. These specific topics are:

- ´Central register of foreigners´ in the country report for Austria;
- ´Population register´ in the country report for Lithuania;
- ´Prison image database´ in the country report for Sweden.

The exceptional country reports are those for Belgium, Ireland and the UK, which have been prepared, based on the data provided in the respective surveys. In addition, open public sources have been used in compiling the report for the UK. Of these three reports, only the Belgium report has been cross-checked and approved by the surveyed authority.

The generalised data (see section ´Generalised data´) is based on the information presented in the cross-checked and approved individual country and organisation reports. This section of the report has not been explicitly verified beyond the TELEFI project team.

Sub-contracting

The legal analysis work for the TELEFI project, to assess the current situation for FR across the EU Members States, was sub-contracted. A public procurement number 208411 ´Analysis of legal regulations related to the enrolment and use of facial images in EU Member States´ was carried out between 08 May and 17 May 2019. The procurement was won by Ernst & Young Baltic AS and the work was performed between 06 June 2019 and 07 February 2020. The respective report ´The Legal Analysis for TELEFI project´ is published as a separate document on the TELEFI project website (www.telefi-project.eu).

Generalised data

1. Facial recognition implementation status in relation to criminal investigations

FR technology has been implemented in 11 EU Member States and in the UK (that left the EU during the study). Additionally, FR has been implemented in 2 international police cooperation organisations (Europol and Interpol). Currently, 7 EU Member States expect to implement FR technology in the next few years (5 Member States during 2021 and 2 Member States during 2022). The remaining 9 EU Member States have given no clear indications of potential FR implementations in the near future. An overview of the FR implementation status, as of December 2020, can be found in Table 1 and Figure 1 below.

Table 1. Implementation status of FR

Country/Organisation	Year of implementation/ expected implementation
FR has been implemented	
Germany	2008
Latvia	2012
France	2013
UK	2014
Slovenia	2015
Hungary	2016
Interpol	2016
Netherlands	2016
Europol	2017
Italy	2017
Greece	2019
Lithuania	2019
Finland	2020
Austria	2020
FR implementation underway	
Croatia	2021
Czech Republic	2021
Romania	2021
Spain	2021
Sweden	2021
Cyprus	2021–2022
Estonia	2022
FR implementation not expected in the near future	
Belgium	-
Bulgaria	-
Denmark	-
Ireland	-
Luxembourg	-
Malta	-
Poland	-
Portugal	-
Slovakia	-

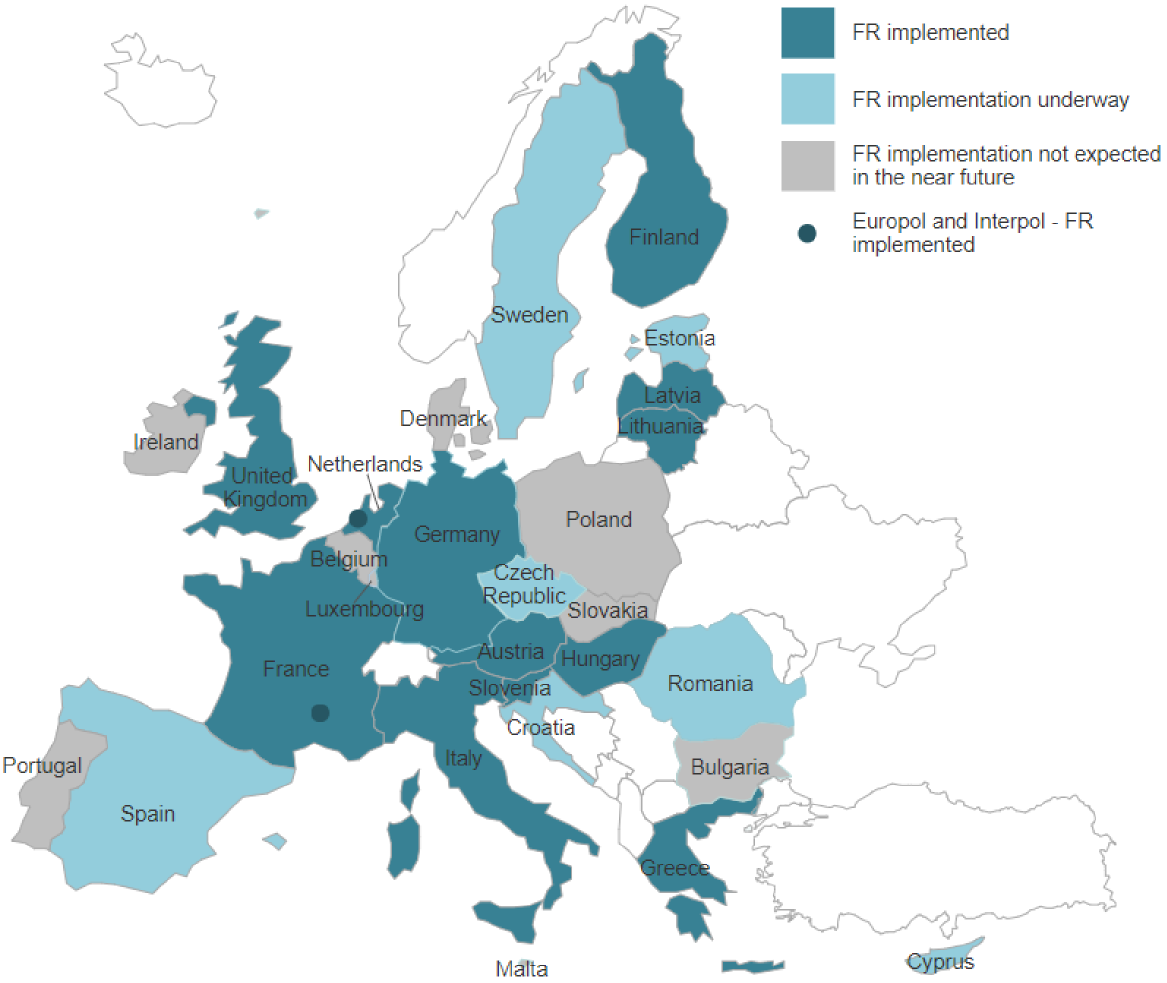

Figure 1. Implementation status of FR

2. EU Member States where facial recognition implementation is not expected to take place in the near future

These are the EU Member States that did not indicate clear plans for the implementation of FR in the next year or two:

- Belgium;
- Bulgaria;
- Denmark;
- Ireland;
- Luxembourg;
- Malta;
- Poland;
- Portugal;
- Slovakia.

Nevertheless, in Portugal, the planning process for introducing FR technology has begun. Despite there being no firm decision for implementation, the most likely scenario is the addition of facial search functionality to the current criminal AFIS and so converting the AFIS system into an ABIS system. The systematic collection of facial images into AFIS, meeting the necessary quality requirements for FR work, was started at 2016. More than 26 000 facial images from around 8700 individuals are stored in the system.

Additionally, the AFIS system in Slovakia contains both fingerprints and facial images, and is considered ready for an upgrade to incorporate FR search functionality.

The main reasons for the non-implementation of FR named by the interviewees are:

- Legal aspects – overall the most common reason (e.g. lack of relevant legislation or legal restrictions that prevent the implementation of FR – named in Belgium, Bulgaria, Denmark, Ireland, Luxembourg and Malta).
- The lack of finance (named in Bulgaria, Poland and Slovakia).
- The lack of demand (named in Poland, Portugal and Slovakia).
- The lack of relevant databases (named in Malta and Poland).
- The lack of political discussion (mentioned in Luxembourg).
- The lack of human resources (named in Poland).

More information about these countries can be found in the sections related to the respective EU Member States.

3. Use cases

The following use cases of FR are addressed:

- Retrospective use (or post-event use or off-line use);
- Live facial recognition;
- “Lights out” scenario.

Where FR has been implemented (in EU Member States, the UK, Europol and Interpol), the most dominant use case for criminal investigation purposes is its retrospective use (see Figure 2). Typically, after a crime has been committed, a facial image of a person of interest (whose identity is unknown and needs to be established) is extracted from a surveillance camera recording during the investigation. This crime scene related facial image (uncontrolled image) is searched using the FR tool against a facial image database that contain images of persons with known identities (controlled images). As a result of the one-to-many (1:N) database search, a list of the best candidates is returned which then needs to be reviewed by a human operator. Based on the human evaluation of any similarities between the image searched (probe) and the images in the candidate list, a decision on the search results (“match”, “no match” or an “inconclusive result”) is made. For reporting purposes, particular phrases are in common use:

- For reporting positive FR results, the terms “potential candidate” or “likely candidate”;
- For reporting negative FR results, the term “no candidate”.

Further, the (positive) search results may undergo forensic one-to-one (1:1) facial image comparisons, usually reported as an expert opinion.

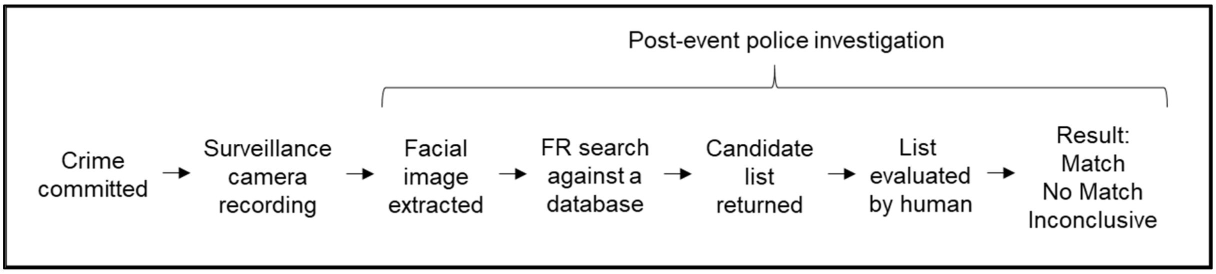
Post-event police investigation
Crime committed
Surveillance camera recording
Facial image extracted
FR search against a database
Candidate list returned
List evaluated by human
Result: Match No Match Inconclusive

Figure 2. Retrospective use of FR

Another retrospective use case is when the police have collected a large amount of image or video material, and want to find a person’s whereabouts throughout all that material. A FR algorithm can be used to find all the images or sequences where a specific face can be found and recognised, saving many man-hours of searching through the material. Of course, this is a trade-off, since there is always the risk that the algorithm may miss an instance of importance, or that the algorithm extracts too many instances such that the follow-up manual review takes an unmanageable amount of effort. It is common that such FR implementations are complemented with object detection and recognition (finding further links using clothes, weapons, cars and number plates).

The second use case of the FR technology is live facial recognition (LFR) (see Figure 3) against a watchlist that consists of facial images of persons of interest (e.g. wanted persons). LFR searches against the watchlist are conducted real-time in a place of interest (e.g. in public spaces such as the street, shopping centres, near sports grounds). Similar to the retrospective 1:N search, a list of the best candidates is returned which is evaluated by a human operator. In case a person of interest is found, the person is approached (immediately) and steps are taken to confirm the identity of the person.

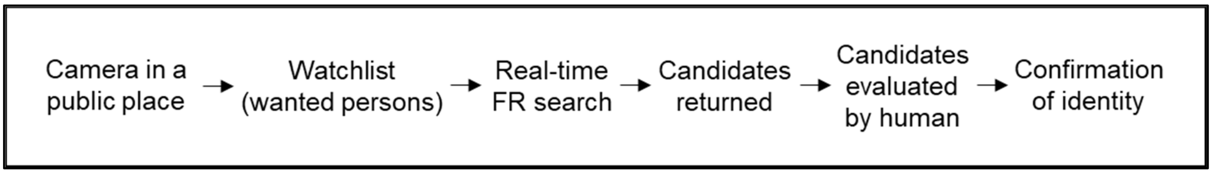

Figure 3. Live facial recognition

Several EU Member States have tested the use of LFR but have not implemented it for routine use. Further, it has not been implemented by Europol and Interpol. To the best of our knowledge, the only police organisation that routinely uses LFR is the Metropolitan Police Service in London, UK.

A third use case of FR technology is fully automated processing without any human involvement. Such an approach is called a “lights out” scenario. It functions using pre-defined score thresholds and has decisions made on “match”/”no match” by the FR algorithm. There were no reports of FR “lights out” being used for criminal investigations from any EU Member State, the UK, Europol or Interpol.

4. Databases

This section presents a general overview of information on databases related to the use of FR in the EU Member States, the UK, Europol and Interpol. It should be noted that only central national databases (with potential for inclusion in the Prüm data exchange) are described, and not local police databases used for FR in some countries. The summarized information is presented in Appendix 3. More detailed descriptions of the databases can be found in the sections relating to the respective EU Member States, the UK and the studied organisations.

As anticipated, remarkable differences exist between the EU Member States, the UK, Europol and Interpol in relation to the use of databases for FR. These differences can be addressed by the following questions:

- Whether the software used for the facial image repository is self-developed or commercial?
- Are facial images stored as part of a larger criminal case management system or in a dedicated database which is used exclusively as a repository for biometric data?
- Are facial images (used for FR) stored only in one or in several databases?
- Do databases contain significant amounts of other information (e.g. fingerprints, biographic data, case data) in addition to facial images?
- What are the person categories from whom the data has been collected and stored in the databases?

The topic is addressed by dividing the information into two subsections:

- Databases used for FR;
- Databases planned to be used for FR.

4.1. Databases used for facial recognition

In Germany and France, self-developed criminal case management systems are used to store the facial images that are used for FR searches. The German database is referred to as INPOL. It contains 5.5 million mugshot images from 6.2 million people from the following person categories: suspects, convicts, arrestees, missing persons, wanted persons and asylum seekers. The French database is known as the Criminal Case History Database (TAJ). TAJ contains 6 million facial images from 21 million individuals from the following categories: suspects and victims (i.e. unknown dead bodies, seriously injured and missing persons). Both databases also store non-biometric information.

In Italy, Greece and Slovenia, commercial software dedicated for storing and searching facial images is used. In Italy, the database is referred to as AFIS, and it stores 17 million facial images (out of which 10 million are FR searchable) from 9 million individuals from the following categories of persons: convicts, arrested suspects, unidentified persons, immigrants and asylum seekers. In Greece, the database used for FR is known as the mugshot database. Data from 377 000 individuals are stored in this database from suspects who have been arrested and from convicts who have been sentenced to imprisonment. In Slovenia, the name of the database used for FR is the Record of photographed persons. It retains data from 110 000 individuals being either suspects, missing persons or unidentified dead bodies. Whilst the AFIS and the Record of photographed persons include non-biometric data, the mugshot database only contains biometric information.

In Finland, Austria and The Netherlands, the facial images that are permissible for FR use are stored in more than one database. In Finland, facial images from suspects are stored in the Registered Persons Identifying Features Database (RETU), which is a section of the National Criminal Database. In addition, facial images collected in Finland from asylum seekers and aliens are entered into the Aliens database. Both databases are self-developed, also contain non-biometric information and can be searched using the face recognition system KASTU. In Austria, the Criminal identification database (EDE) and the Central register of foreigners (IRZ) are the two databases that can be legally used for FR during criminal investigations. However, technically, it is currently possible to search only EDE. EDE is a self-developed database, where information needed for identification is stored. EDE is linked to several sub-databases including the Database of images of criminals, missing persons and dead bodies. EDE contains 1.25 million photographs of 620 000 known individuals. In The Netherlands, a FR system called the Central Automatic Technology for People Recognition (CATCH) is used in order to perform facial searches during criminal investigations. FR searches can be performed in two physically separated databases – CATCH criminal and CATCH alien. CATCH criminal contains facial images from suspects and convicts, whilst CATCH alien holds information derived from the core database for foreigners about visa and asylum applications. The number of individuals whose data is stored on CATCH criminal is 1.3 million (with 2.2 million images, respectively), whereas the number of individuals stored on CATCH alien is 7 million. The CATCH databases contain solely biometric data with references to the relevant metadata.

In Lithuania, a database called the Habitoscopic Data Register (HDR) is used for FR searches. This self-developed database is part of an information system that stores information about the appearance of people, including photographs. More than 400 000 facial images from 185 000 individuals being either suspects, convicts, arrested persons, wanted persons or unidentified dead bodies and unidentified helpless persons are entered into HDR together with non-biometric information.

In Latvia and Hungary, a central biometric data repository is used for the data collected by the state. The Latvian Biometric Data Processing System (BDAS) runs on commercial software and consists of several logically separated datasets, one of which is the criminal data array. The criminal data array of BDAS contains information on 270 000 cases of which 78 000 include facial images. Facial and fingerprint data from detained, suspected, accused and convicted individuals and, unidentified dead bodies are entered into the criminal array of BDAS, together with non-biometric information. Only facial data in the criminal array of BDAS can be searched during criminal investigations. In Hungary, the Facial Image Registry also runs on commercial software. The Facial Image Registry is synchronised with several source databases where the biometric and non-biometric information is first entered during different document/civil proceedings. The Facial Image Registry only contains facial images, facial image templates and references to the source data. About 30 million templates from individuals of known identity are stored in the Facial Image Registry and are searched during criminal investigations.

In the UK, the central national searchable facial image database is the Police National Database (PND) containing 14–16 million images. PND is an intelligence system linking regional police forces in the UK. It was developed by the UK Home Office in cooperation with a commercial company. Facial images collected by regional police forces, first stored in local police databases, are subsequently uploaded to PND and can then be searched by all regional police forces. A few local police databases have FR search capabilities of their own.

International police cooperation organisations, Europol and Interpol, also perform FR searches and have databases that contain facial images. In Europol, there are two divisions that use the FR technology – the European Counter Terrorism Centre (ECTC) and the European Cybercrime Centre. This report presents the data gathered from ECTC that owns a database called FACE. The database used for FR searches in Interpol is called the Interpol Face Recognition System (IFRS). The Europol and Interpol databases contain information sent by the countries that have cooperation agreements with these organisations. IFRS stores facial information for 80 000 individuals. The number of individuals with images stored on FACE was not reported.

4.2. Databases planned to be used for facial recognition

The implementation of FR is currently underway in 7 EU Member States. These Member States are Sweden, Spain, Romania, Czech Republic, Cyprus, Croatia and Estonia. Each has a plan about the database(s) to be used for FR work. These plans are introduced in this subsection.

Commercial multibiometric systems to store and search facial images as well as fingerprints are planned for FR in Sweden, Spain, Czech Republic, Estonia and Croatia. Additionally, in Croatia, an image repository of civil documents will include a FR search capability. A dedicated database for storing facial images for FR use in Romania has been developed in-house, known as the National Biometric Identification System (NBIS). In Cyprus, facial images planned for FR use are stored in a database referred to as ISIS Faces, running on commercial software.

In Sweden, facial mugshot images are currently stored in a mugshot database with a plan to transfer them to ABIS in 2021. The digital mugshot database in Sweden contains 60 000 data entries of suspects and convicts. FR functionality in ABIS is expected to be operational in 2021.

In Spain, there are several separate mugshot databases owned by different police forces across the country, with altogether 5.6 million images from 3.9 million arrested persons. AFIS that is currently used for fingerprints will be converted into ABIS and populated with facial images stored in the separate mugshot databases. FR functionality in ABIS is expected to be operational in 2021.

In Czech Republic, FR in CBIS is expected to become operational in 2021. CBIS will be populated with facial images from a database called FODAGEN, which contains fingerprints and photographs of suspected, accused and convicted persons. The number of person records in FODAGEN is between 200 000 and 300 000.

In Estonia, a central ABIS system is expected to be launched in March 2021. It will be used for storing fingerprints and facial images collected by the state during criminal and civil proceedings. The data in ABIS will be logically separated into the criminal and civil subsystems, while the criminal subsystem will primarily be used for FR searches in criminal investigations. Collection of facial images and their entry into the criminal subsystem of ABIS from suspected, accused and convicted persons is planned to start in 2022.

In Croatia, two databases with facial images are going to be used for FR searches in criminal investigations. These are ABIS and the image repository of civil documents. The ABIS is used for storing fingerprints and facial images collected from suspected, accused and convicted persons. It contains data on 220 000 individuals. The image repository of civil documents is used for storing facial images collected during the issue of ID cards, travel documents and driver's licences. It contains 18 million images from 5.7 million individuals. FR search functionality is expected to be available in these databases in 2021.

In Romania, the NBIS database has been used since 2016 for storing facial images but, so far, without the FR search functionality. It contains information on 300 000 individuals from the following categories of persons: suspects, convicts, unknown persons, missing persons and unidentified dead bodies. FR is expected to be implemented in 2021.

The ISIS Faces database used in Cyprus holds facial images of 2000 convicted persons and the FR functionality is expected to be operational in 2021 or 2022.

5. Data acquisition

This section presents a general overview of data acquisition related to the use of FR in the EU Member States, Europol and Interpol.

Facial images that are used for FR in criminal investigations, are stored in two classes of database:

- Criminal databases – databases that are established with the aim to solve crimes;
- Civil databases – databases that are established with the aim to manage the data collected during different civil proceedings (e.g. issuing ID cards, driver's licences and databases relating to aliens).

The data acquisition for civil databases varies significantly between the authorities collecting the data in EU Member States. For this reason, generalisation of this information was not possible.

However, the data acquisition process for criminal databases involves many common aspects. Typically, the facial images are captured by police forces across the country. The number of premises where the images are taken and the number of police officers who perform this work is large. As a rule, the biometric and non-biometric data are collected in parallel. Often, the process starts with the recording of biographic information and is followed by the collection of biometric data – facial images, fingerprints and, if applicable, DNA. Also, as a rule, the identity of the individual whose data is collected is checked during the acquisition process, either against an identity document or against previously stored biometry (e.g. mostly against fingerprints). In most EU Member States, the data is entered directly into the respective database(s) by the authority performing the acquisition. However, in some Member States such as The Netherlands, Greece, Sweden, Cyprus and Croatia, the data are not entered into the database(s) by the authority performing the acquisition. For instance, facial images are collected at 400 police units across The Netherlands and are sent to the Centre for Biometrics and entered into the CATCH criminal database by trained face experts. In Greece, mugshot images are taken either at the Hellenic Police Forensic Science Division or in 70 police stations across the country, but in both cases, the image entry into the mugshot database is performed by the forensic examiners at the Hellenic Police Forensic Science Division. In Sweden, images, fingerprints and other data are collected by police officers at booking stations and sent to the National Forensic Centre for entry into the mugshot and AFIS databases. In Cyprus, images are taken by police photographers across the country, but are entered into the ISIS Faces database centrally by the personnel of the Criminalistic Services. In Croatia, facial images are entered into ABIS by forensic technicians at the Forensic Science Centre "Ivan Vučetić". The same general principle is relevant for Europol and Interpol that do not capture any facial images, but receive the images for entry into their databases from the countries that have cooperation agreements with these organisations. The data is entered by the accredited Europol officials and the Interpol officers.

More detailed descriptions of the data acquisition can be found in the sections related to the respective EU Member States and the studied organisations.

6. Requirements for facial images

This section presents a general overview of image requirements related to facial image databases in the EU Member States, Europol and Interpol. It should be noted that only data from the EU Member States where FR has been implemented, or soon will be implemented, are described. The summarized information is presented in Appendix 4.

As with the previous topic, facial images used for FR in criminal investigations, are stored in two classes of databases:

- Criminal databases – databases that are established with the aim to solve crimes;
- Civil databases – databases that are established with the aim to manage the data collected during different civil proceedings (e.g. issuing ID cards, driver's licences and databases relating to aliens).

The requirements for facial images acquired for civil databases vary significantly between the EU Member States and authorities involved in the image acquisition process. However, the following two principles are common in most Member States:

1) Facial images are generally captured as frontal views;
2) Facial images are generally captured according to the ICAO standard.

Regarding criminal databases, the requirements for facial images and the practices used for quality assurance also show significant variations. However, these databases do share more common aspects relative to the comparison for civil databases.

Frontal view facial images are entered into the database(s) for all EU Member States where FR has been implemented (or will be implemented in the near future), for Europol and for Interpol. In 4 Member States (The Netherlands, Lithuania, Latvia and Hungary) and Interpol, frontal view images are the only image types entered into the database(s) whereas most Member States store images with several different views. Most typically, these different images are one or both side views and one or both half-side views. In addition, images of full body, special marks, scars and tattoos can be stored.

Other than the following 5 EU Member States, no others declared any quality standards for image capture and/or database entry. Quality standard are applied by the following Member States:

- The Netherlands (CATCH criminal) – SOP for data acquisition follows ISO/IEC 19794 standard;
- Germany (INPOL) – images are stored in accordance with ISO/IEC 19794-5 standard;
- Latvia (criminal data array of BDAS) – facial images must correspond to the requirements of ANSI/NIST ITL-1:2011 and ISO/IEC 19794-5 Part 5: Face image data;
- Hungary (Facial Image Registry) – all photographs are taken in accordance with ICAO and ISO/IEC 19794-5 standards;
- Romania (NBIS) – facial images are captured according to ICAO 19303 and ISO/IEC 19794 standards.

Despite the fact that most EU Member States do not apply quality standards for image capture and/or database entry, most have written SOPs for performing these tasks. Further, two-thirds of the EU Member States, declared to have a training process in place for personnel performing the named tasks.

Quality control over facial images, if applied, is performed either by human intervention or automatically by the software.

The most common file format being used for image storage is JPEG, but several other formats are also used such as PNG, BMP, GIF, TIFF and JPEG/JFIF.

More information about the quality requirements and assurance can be found in the sections related to the respective EU Member States and the studied organisations.

7. Facial recognition searches

This section presents a general overview of how FR searches in the central national databases are performed in relation to criminal investigations in the EU Member States where FR has been implemented. In addition, information about the FR searches performed by Europol and Interpol is presented. Information about FR searches is also presented in Appendix 5. This section does not include information relating to the EU Member States where implementation of the FR technology is currently underway, nor about the UK.

Commercial software is being used for FR searches in all EU Member States, regardless of whether the facial image database is commercial or has been self-developed. The same applies for Interpol. The only exception is Europol, where the FR software has been developed in-house and is based on open-source components.

Typically, the frontal image view is the controlled image against which FR searches are performed. Additionally, in Austria, searches are performed against the half-side view stored in the database.

Depending on who perform FR searches, the EU Member States can be divided into two groups:

1) Member States where FR searches are performed by a limited number of specialists, who perform searches for all authorities that make requests;
2) Member States where a wide range of police officers are allowed to perform FR searches and perform those searches as part of their ongoing investigations.

The EU Member States where there are a limited number of specialists in the facial field performing FR searches: Germany, Greece, Slovenia, Austria, The Netherlands and Hungary. The same practice is followed by Europol and Interpol.

The EU Member States where there are a wide range of police officers performing FR searches are: France, Italy, Finland, Latvia and Lithuania.

The FR search results are returned as a list of candidates. In most instances, the candidate list is reviewed and evaluated by the person who performed the search. The number of candidates in the list varies between the EU Member States ranging from 10 to 1000. In addition, there are differences between the Member States regarding whether the candidate list can include only one image for a given individual (the most likely one) or more than one, if several images for the individual are stored in the database.

Typically, the FR search results are used for operational purposes to support an investigation and the search results are not suitable for presentation as evidence in court. This practice is followed in: France, Italy, Slovenia, Finland, Austria, Lithuania, Latvia and Hungary. Similarly, the searches performed by Europol and Interpol are meant to be used for intelligence and not as evidence in court. Nevertheless, there are Member States (Germany, Greece and The Netherlands) where, in certain circumstances, the FR search results can also be used as evidence in court.

Training to perform FR searches, is either thorough, basic or the training availability has not been specified. Understandably, extensive training programmes are easier to apply in Member States where the number of specialists performing facial searches is limited.

The existence of written methods/guidelines for FR searches is an exception rather than a rule. To the best of our knowledge, no proficiency testing has been developed for the FR field. In contrast, manual 1:1 facial image comparison has proficiency testing on a yearly basis via the ENFSI DIWG.

Some EU Member States provided statistics on the use of FR. The number of FR searches performed is greatest in France – 200 000 in 2018. Germany is next with 53 000 searches in 2019. The number of searches in The Netherlands was 1048 in 2018. In Slovenia, the annual number of searches is between 150–200. The reported match rate for searches ranged from 1% to 8.2%.

More information about the FR searches can be found in the sections related to the respective EU Member States and the studied organisations.

8. Use of facial images collected for non-criminal purpose in criminal investigations

In general, the databases used for FR in relation to criminal activity are established explicitly with the purpose to store and process facial images collected during criminal investigations. There are a few exceptions where non-criminal databases, containing facial images, can be used for FR in crime investigations:

- In Hungary, the only database used for FR in criminal investigations is the Facial Image Registry that contains facial images collected for various document applications.
- In 3 EU Member States (Austria, Finland and The Netherlands) two databases are legally permissible for FR use in criminal investigations. One of these databases is a criminal database and the other is related to foreigners. At the present time, the foreigner's database in Austria (IZR) is not connected to the FR system and, thereby, is not searched. The databases related to foreigners in Finland and The Netherlands are available for FR searches. The Finnish database (Aliens database) contains facial images from asylum seekers and other non-Finnish citizens. The individuals who search the Finnish Aliens database need additional training and extra permissions. The Dutch database (CATCH alien) contains facial images from Visa and asylum applicants. Searches in the Dutch CATCH alien for criminal investigations are only

permitted with a written order from the prosecutor and with the consent of an investigating judge.

- In Croatia, where FR is expected to become operational in 2021, searches of two databases are planned in criminal investigations. One of them is ABIS, which is a criminal database and the second one is the image repository of civil documents, which is a common repository used for the storage of facial images obtained during the issue of ID cards, passports and driver's licences.
- In Estonia, where FR is expected to become operational in 2022, the criminal and civil biometric data collected by the state will be stored (logically separated) in the ABIS database. Primarily, the facial images in the criminal part of ABIS will be searched. However, it is likely that in serious crime, with special permission from a prosecutor, the search will be allowed in the civil part of ABIS.

In addition, some criminal databases hold facial images from categories of persons that are not included directly for the purpose of solving crimes:

- INPOL in Germany stores facial data on missing persons and asylum seekers.
- TAJ in France stores facial data on missing persons and unidentified dead bodies.
- AFIS in Italy stores facial data on asylum seekers and immigrants. 90% of the AFIS subjects are foreigners.
- The Record of photographed persons in Slovenia stores facial data on missing persons and unidentified dead bodies.
- EDE in Austria stores facial data on missing persons and unidentified dead bodies. However, FR searches for identification purposes are not performed.
- HDR in Lithuania stores facial data on unidentified dead bodies and foreigners detained for illegal trespassing at the state border.
- The criminal data array of BDAS in Latvia stores facial data on unidentified dead bodies.
- NBIS in Romania stores facial data on missing persons and unidentified dead bodies.

The summarized information is presented in Appendix 6.

Other than the previously described cases, where facial images collected for non-criminal purposes are used in criminal investigations, the facial images collected and stored for civil purposes (i.e. in the course of various document applications) are not allowed to be used for FR in criminal investigations. Nevertheless, in most countries, the police can request such images for manual 1:1 facial image comparisons.

9. Uncontrolled images

Typically, the facial image databases used for FR in criminal investigations, contain controlled images and the storage of uncontrolled images in these databases are less common (see Appendix 7). Nevertheless, there are some EU Member States that do store uncontrolled images or plan to start storing such images.

The EU Member States that do not store uncontrolled images in the FR database: Italy, Greece, Finland, the Netherlands, Lithuania, Latvia and Hungary.

The EU Member States that can store uncontrolled images in the FR database: Germany, France, Slovenia and Austria.

No EU Member State where FR implementation is underway, currently stores uncontrolled images in the database planned for FR use.

Regarding Europol and Interpol, both store uncontrolled images, which are included in their databases.

10. Legal framework

Legislation related to the use of facial images for criminal investigations by the EU Member States were studied through:

- The legal analysis performed by Ernst & Young Baltic AS;
- The dedicated questions addressed during the TELEFI project interviews.

The results of the legal analysis are published in the report ´The Legal Analysis for TELEFI project´ that can be found on the TELEFI project website (www.telefi-project.eu).

Information from the end-users (if provided during the interviews) can be found in the sections related to the respective EU Member States.

11. Prüm

In this section, the views of the interviewees from 27 EU Member States regarding the potential inclusion of facial images into Prüm data exchange and about the potential Prüm architecture for facial image exchange are summarized. It should be noted that the views presented may not necessarily represent the official views of the interviewed authorities neither the official views of the EU Member States.

11.1. Inclusion of facial images to Prüm data exchange

Interviewees from 20 EU Member States expressed a positive view on the potential inclusion of facial images into Prüm data exchange. Interviewees in 1 Member State expressed mixed feelings on this topic. Interviewees from 4 EU Member States preferred not to express their views. No interview answers were received from 2 EU Member States (categorised under "No opinion expressed"). None of the interviewees expressed a negative view on the inclusion of facial images into Prüm data exchange.

Table 2. Inclusion of facial images to Prüm data exchange

	Positive	Mixed	Negative	No opinion expressed	TOTAL
Countries where FR has been implemented	9	0	0	2	11
Countries where FR implementation is underway	4	1	0	2	7
Countries where FR implementation is not expected in the near future	7	0	0	2	9
TOTAL	20	1	0	6	27

Additional opinions/concerns raised by the interviewees:

- Although it is highly likely that facial images in Europe will be exchanged within the Prüm framework, it will take a long time until it involves all EU Member States. Firstly, this is because Member States are currently at very different levels regarding the implementation of FR technology (less than half the EU Member States) and the development of national facial image databases for this purpose. Secondly, the experience from the exchange of fingerprints and DNA has shown that it takes more time for the Member States to become operational than expected.
- Decisions are required as to who can perform the Prüm facial image searches. In contrast to fingerprints and DNA, that are searched by a limited number of specialists,

FR searches in some EU Member States are performed by a wide range of police officers and not only by face experts. This is the case in 5 out of 11 Member States where FR for criminal investigation has been implemented. In these countries, it is inevitable that there will be a need to scale down the number of individuals that have permission to perform the Prüm searches.

- In some EU Member States, it was stated that although the addition of face modality to the Prüm data exchange is a good idea, it will only be fully approved by the Member States after agreement has been reached on important technical aspects.

It can be concluded that in most of the studied EU Member States (74%), the interviewees expressed a clear positive attitude towards the extension of the Prüm system to add facial images and that no clear opposition on this matter was expressed. Furthermore, the views did not depend upon whether or not FR was already being used in the specific Member States.

11.2. Prüm architecture for facial image exchange

Interviewees from 12 EU Member States were in favour of the current decentralized architecture, where each country is the owner of its data and the exchange of facial images with other countries works in a bilateral way. A centralized solution, where facial images in national databases would be synchronised to a central European database, was favoured by the interviewees from 5 EU Member States. Interviewees from 4 EU Member States either, did not have a clear preference, or favoured the development of an intermediate solution between the centralized and decentralized model. Interviewees from 4 EU Member States preferred not to express their preferences on the potential Prüm architecture. No interview answers were received from 2 EU Member States (categorised under "No opinion expressed").

Table 3. Prüm architecture for facial image exchange

	Centralized	Mixed	Decentralized	No opinion expressed	TOTAL
Countries where FR has been implemented	2	1	5	3	11
Countries where FR implementation is underway	2	1	3	1	7
Countries where FR implementation is not expected in the near future	1	2	4	2	9
TOTAL	5	4	12	6	27

Additional opinions/concerns raised by the interviewees:

- Interviewees from some EU Member States had very strong positions in favour of the decentralized solution and presented a number of arguments in support. A very significant statement was that bilateral data exchange, where the biometric data of known individuals stays in the national database and is not sent out of the specific country, is considered to be the only practical solution that would work for data exchange, when the EU legal landscape is taken into account. Furthermore, a view was expressed that the quantities of data in national databases will always be greater than the quantities of data that the EU Member States will send to a central European database. Thereby, the probability of getting true matches during the data exchange will be much higher if the data is kept in the national databases and is searched bilaterally. In addition, the flexibility and efficiency of local systems and their capability for expansion were much higher when compared to a large centralized European system.

- Interviewees in most EU Member States, considered the centralized approach to data exchange, technically less complicated and easier to implement compared to the situation where databases in 27 EU Member States would need bilateral connectivity.
- If a centralized architecture became an option, it was suggested that Europol might have a coordinating/monitoring role in maintaining the central database.
- It was suggested that not all the images in national databases be included in the data exchange, but only the ones related to the most serious international crimes. It is thought that sending such images to the central database would not be a legal problem for most EU Member States.
- If a decentralized model was adopted, it is anticipated that it will be very time consuming to manually analyse all the candidate lists from all the countries separately. It was suggested that all the facial images from the search results in different countries might be re-analysed by a central FR engine which then delivers a single candidate list to the requesting country.
- Centralized European databases (e.g. Schengen Information System, Visa Information System, Eurodac etc.) as well as decentralized databases of the EU Member States (e.g. Prüm, Passenger Name Record etc.) are all considered valuable tools that meet separate, but complementary operational needs.

It can be concluded that in more than half of the studied EU Member States (57%) where the interviewees expressed a view about the Prüm architecture, the current decentralized Prüm architecture was favoured. Furthermore, the views did not depend upon whether or not FR was already being used in the specific Member States.

12. Harmonization of facial recognition field at the European level

Interviewees from 20 EU Member States (74%) were positive about the harmonization of the FR field at the European level. The positive responses varied on a scale from "'would be beneficial" to "inevitable". Interviewees from 2 EU Member States (both using FR) did not consider the European-wide harmonization to be necessary. No opinion on the harmonization topic was expressed by the interviewees from 3 EU Member States. No interview answers were received from 2 EU Member States (categorised under "No opinion").

Table 4. Attitude towards the need for harmonization of the FR field at the European level

	Positive	Negative	No opinion	TOTAL
Countries where FR has been implemented	8	2	1	11
Countries where FR implementation is underway	5	0	2	7
Countries where FR implementation is not expected in the near future	7	0	2	9
TOTAL	20	2	5	27

For the 2 EU Member States that did not consider harmonization to be necessary, it was considered that there would not be any benefits from having a common FR EU-guideline for those countries or organisations that have already implemented FR. Moreover, it was stated that it is not always possible for the police to achieve high quality images and the law enforcement agencies must work with all the images that they have available. A concern was expressed that if European standards were set, some images will be left out from the databases. It was considered sufficient to apply national rules and that all Member States must have the right to decide for themselves which images are held in their databases and which images are searched. It was noted that the fingerprint data exchange between EU Member

States works very well without having common standards applied across Europe and therefore it should also work well with facial images.

In summary, most of the interviewees were in favour of European level harmonization. It was admitted, that although harmonization is necessary, it will be a complicated task and a common standard for FR databases will be difficult to put into place. Moreover, it might be time-consuming and costly to implement a standard within most EU Member States. Achieving harmonization, although beneficial, will represent a challenge, since countries are using different technologies and different methods. But, despite the problems, many benefits were envisaged through having a common FR EU-guideline and its topics should include the quality of images, how to pre-process probe images, how to analyse candidate lists and, how to report the results. An EU-guideline for FR could greatly improve the quality of the international data exchange.

Recommendations for the EU Member States

1. Recommendations towards the harmonization of the facial recognition field at the European level

Recommendations for harmonization are primarily given in the context of potential international facial image exchange.

1) EU Member States should make joint efforts towards the European-wide harmonization of the facial recognition field. In the first instance, the harmonization should focus on six topics:
    - Agreement on the standard and quality requirements for controlled images;
    - Development of recommendations for FR search methodology;
    - Development of recommendations for training human operators;
    - Development of proficiency tests for 1:N searches;
    - Development of recommendations on reporting;
    - Development of common terminology.

2) Considering the vision for interoperability, both criminal and civilian specialists in facial biometrics would benefit from a joint harmonization process in terms of facial image quality standards, database management, manual facial comparative methods and candidate list review methodology.

3) A forensic working group consisting of specialists from the EU Member States should be set up for the coordination of the harmonization process. It should work in close collaboration with the ENFSI DIWG and other EU working groups/organisations (e.g. Europol) involved in the topic. The DIWG has already initiated work on a guideline for FR searches and is providing annual proficiency tests on manual 1:1 facial image comparisons.

4) Quality recommendations should be based on the following quality standards:
    - Facial image capture methodology – ISO/IEC 19794-5:2011 - corrected version 2016, Information technology - Biometric data interchange formats - Part 5: Face Image;
    - Facial image quality – ISO/IEC TR 29794-5:2010 Information technology - Biometric sample quality - Part 5: Face image data;
    - Methodology for FR searches, should be standardised in the long term according to e.g. ISO 17025 or ISO 21043.

5) Establish a large European dataset of facial images to be available for future FR work in the criminal field, for specific purposes:
    - Research and development;
    - Testing of FR software during a tendering process and on a regular basis after its implementation;
    - Training of human operators;
    - Proficiency tests.

2. Recommendations towards the Prüm exchange of facial images

1) The results of the project provide further support for the introduction of the face modality into the Prüm data exchange.

2) In order to speed up the introduction of the face modality into Prüm, the facial image exchange should be first implemented using the current decentralized Prüm architecture. The preference towards the centralized solution, could lead to a considerable delay in the Prüm extension because of the legal and privacy issues that are seen to prevent the sending of biometric data from national databases to a central European database.

3) In parallel with the implementation of the decentralized solution, it is recommended that work continues on a potential move towards the centralized solution. This work should initially focus on understanding whether it is possible for all EU Member States to send biometric data of known individuals to a central European database, taking into account the possible legal obstacles and privacy issues.

4) Reach an agreement amongst all EU Member States that Prüm facial image searches will be performed by a limited number of trained specialists in each Member State.

5) Reach an agreement amongst all EU Member States on an interoperable process for performing Prüm facial image searches and on a harmonized approach for the interpretation of the search results.

6) Initiate discussions as to whether it is possible to enhance the bilateral searches that arise from the decentralized solution, through combining all the images received from the different countries into a single list of ranked candidates.

7) Increase flexibility options for the countries requesting/performing Prüm searches. This should include control over the number of candidates returned in the search results. In the case of bilateral searches, it should also be possible to decide in which countries the search is performed. Further, no common threshold should be applied because of the different systems used in different countries.

Country reports

Austria

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

FR has been implemented in Austria since August 2020.

Amendments to the laws that enable the use of FR for the detection and prevention of crime were adopted in March 2016. The creation of the legal basis was followed by a procurement process that resulted in the purchase of a FR system in October 2018. Since then, numerous tests were conducted with tens of thousands of images to establish the suitability of previously collected images for FR searches. A test-pilot for the use of FR in criminal investigations ran from November 2019 until the end of June 2020. During the pilot, facial images from 581 criminal cases were searched and processed. In 83 criminal cases (14.3%), a positive search result for the potential offender was obtained using the FR system. Years of preparation and the positive test results have provided a sound foundation to move ahead with operational FR in 2020.

The database that is connected to the face recognition system is known as the Criminal identification database. This includes images from criminals, missing persons and dead bodies, as well as crime scene images (i.e. uncontrolled images). As of September 2019, about 1 250 000 photographs of 620 000 known individuals were stored in the database, while the number of uncontrolled images was less than 1000.

Currently, FR in criminal investigations is implemented at a central unit of the Criminal Intelligence Service of Austria. FR searches are performed by three qualified specialists of the Criminal Intelligence Service. The search results can only be used for investigative purposes.

During the second phase of implementation, the FR technology will be expanded to the provincial level, i.e. to the 9 provincial criminal investigation departments of Austria. Thereafter, most of the FR work will be carried out at this level and only the most serious crimes will be dealt with in the central unit of the Criminal Intelligence Service in Vienna. When FR at the provincial level has been implemented, it should become clearer over time whether there is a need to proceed further and implement it at district level across the provinces.

According to Austrian legislation, FR searches for criminal investigation purposes are also permitted within the Central register of foreigners, which is essentially a civil database. However, this database is not connected with the FR system and, thereby, not searched at the present time.

It is not permitted to perform FR searches for crime investigation in other civil databases such as in the Identity documents register, the Social security register and the Driver's licence database. Nevertheless, the police can request images from these databases.

1.2. Organisations involved

The Criminal Intelligence Service of the Federal Ministry of Interior of Austria is responsible for the implementation and use of FR in criminal investigations.

1.3. Databases that contain facial images and are permitted to be used for facial recognition in relation to criminal activity

Legally, two databases in Austria can be used for FR searches for the detection and prevention of crime:

- Criminal identification database ("*Erkennungsdienstliche Evidenz*", EDE);
- Central register of foreigners ("*Integriertes Zentrales Fremdenregister*", IZR).

Both of these databases are owned by the Federal Ministry of Interior (database custodian and processor). However, the owners and controllers of the data are the regional police or regional foreign authorities that entered the data into the respective databases. Currently, only the Criminal identification database is connected and searched with the FR system.

1.3.1. Criminal identification database

The Criminal identification database (EDE) contains personal data, additional information on criminal offences, and a date when and by whom biometric data (fingerprints, facial images and DNA) were collected. EDE is linked to other identification sub-databases including biometric ones. There are four databases in the Austrian police that contain biometric data:

- DNA database (DNA profiles from stains, and criminals, missing persons and dead bodies);
- Fingerprint database (AFIS, dactyloscopic data from open crime scene cases and finger- and palmprints from criminals, missing persons and dead bodies);
- Database of images of criminals, missing persons and dead bodies;
- Database for crime scene images.

All the above-mentioned databases (except the AFIS search system) have been developed locally in Austria, mainly by software engineers at the Ministry of Interior.

Biometric and non-biometric data are always collected in parallel during a process, which starts with the recording of personal data and crime case data (e.g. name, date of birth, citizenship, ID document, description of a person, reason for an acquisition etc.). Photographs are then taken. The photography is followed by the collection of fingerprints. The collection of this dataset is allowed in case a person is suspected of committing an intentional criminal offence. Finally, DNA is collected if the punishment of the crime can be at least one-year imprisonment. After the acquisition, biometric data is enrolled automatically into the respective national databases and, if possible, also checked against international biometric identification databases in a systematic manner (e.g. Prüm DNA and Prüm AFIS network, SIS AFIS, PCSC USA AFIS). The data collected, is always checked against previous records by the persons working with these databases. Also, civil registers (e.g. the Birth register and the Identity documents register) can be used during the data verification procedures. If the data is obtained from a foreign citizen, data requests are made to the registers of other countries for verification purposes (via Interpol channels and with transmission of fingerprints and photographs to the country of citizenship).

Images are captured and stored in the database from accused and convicted persons who are older than 14 years of age and if the crime was committed intentionally. The following images are taken:

- Front view facial image;
- Right side view facial image;
- Left half-side view facial image;
- Full body photo (frontal view, starting from 2004);
- Photographs of special features and tattoos.

Photographs are taken with professional digital reflex cameras and sent to the database using an IT solution developed by the Austrian police. Webcams or image capturing stations are not used. Currently, the resolution of images is 960 x 1280 pixels. There must be at least 32 pixels between the centres of the eyes in order to perform a FR search (this requirement is set by the FR software).

Photographs of known persons (i.e. controlled images) are taken by police officers in 180 police stations across Austria or in units for asylum seekers. If photographs from a known person have been taken at different times, all images are retained in the database. A new photograph should be taken if six months or more has passed since the last image was captured or if the appearance of the person has changed considerably.

Images of the person can be stored in the database until the person reaches the age of 80 years, but not for less than five years. However, data can be removed from the database before the above-mentioned deadline on the request of the person in situations where further data processing is no longer necessary (e.g. there is no reason to fear the person will commit criminal offences). The request is first reviewed by the police and then, if the request is refused, the person may appeal to the data protection authority, whose rulings are binding on the police. As of September 2019, the database contained about 1 250 000 images for 620 000 known individuals.

Crime scene images (i.e. uncontrolled images) can be stored in the database for up to 60 years, depending on the type of crime and on court decisions. In any case, such images must be deleted after a crime case is closed. The number of uncontrolled images as of September 2019 was less than 1000. It is anticipated that the number will grow rapidly now that the implementation of FR technology has been completed. In addition to these images, related information such as location of the crime scene, time of crime, names of police officers working with the case etc. are stored in the database.

1.3.2. Central register of foreigners

Foreigners over 14 years of age are registered in the Central register of foreigners (IZR) under the circumstances listed below:

- In case of illegal migration or an illegal stay in Austria;
- If applying for permission to live in Austria;
- If applying for a work permit;
- If the person has submitted an asylum application in Austria.

IZR contains about 5 million datasets. There may be more than one dataset per person. As a rule, all persons are photographed with one or more images per person. There is no limit to a number of images that can be stored for each person. If an image of an individual is enrolled several times, all images are retained in the database. In most cases, facial images are captured and enrolled by police officers at police stations. The data can also be collected and enrolled by migration officers and asylum officers. Digital cameras are used for facial image capturing and the requirements for the cameras are described in a best practice manual.

There is a wide variety in the types of photograph captured for individuals (frontal view, side view) as well as significant quality variation.

Other personal data (e.g. name, age, gender, legal status whether allowed to stay in the country or not) and fingerprint data are stored for each individual whose image is enrolled. The identity of a person is checked against previous entries in the databases using fingerprints.

Facial images are retained in the database for as long as the dataset for the person is held in the database. The dataset is removed from the database if a person dies, becomes an Austrian citizen or ten years has passed since the data was last edited.

1.4. Facial recognition searches

The search engine for FR was purchased from the Cognitec company and was implemented by the IT company Atos.

FR searches are performed using images stored in the Criminal identification database. Both, front and half-side images in the database can be used for the searches.

The FR search process involves investigators sending probe images of unknown criminals to the Criminal Intelligence Service, thus initiating a manual search against the database. Any police authority entrusted with the investigation or prevention of a judicial offence will be permitted to request a FR search. No permission from a prosecutor or court will be required for this to happen. The search conducted by the Criminal Intelligence Service will result in a list with 30 candidates with the 10 highest ranking candidates forwarded to the investigating officer. The list contains an image of the candidate, a match value (in percent) and a reference number to the Criminal identification database, where further information on the given candidate can be found. The candidate list contains one image per person (the one with the highest match value) even if several images of the same person are held in the database.

FR searches are used only for investigative purposes and not for the identification of unknown criminals or dead bodies.

1.5. Quality assurance

The following measures have been applied to ensure the quality of the images collected from individuals:

- First level – training of personnel who capture the images. All police officers who take photographs have undergone special training for the collection of biometric data.
- Second level – best practice manual. The best practice manual is issued to police officers collecting biometric data and it is called ‘Provision for Biometric Identification’.
- Third level – centralized quality checks. Quality checks of the photographs taken are performed centrally in the Criminal Intelligence Service of the police. If quality problems are observed, the relevant police authorities are informed and the collection of the data must be repeated. A poor-quality image can still be enrolled and stored in the database but it will not be searchable using the FR system.

Dactyloscopic examinations and DNA examinations in Austria are accredited according to EN/ISO 17025. Accreditation in the area of FR is not planned at the present time. This is because FR will only be used to aid in criminal investigations and the search results will not be used for expert opinions.

The quality of crime scene images (i.e. uncontrolled images) is checked when FR searches are performed. They must be sufficient for making templates. The compliance of images with the quality requirements for the FR system are checked automatically by the software. At the present time, no further quality requirements for the uncontrolled images have been specified because more experience of using the FR system is still required.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The legislative acts that regulate the use of biometric data (including facial images) by the law enforcement agencies are:

- Security Police Act (Ministry of Interior is responsible for the law), § 64-79;
- Data Protection Law;
- Federal Law on Foreigners and Asylum (BFA-VG), § 27-32;
- Code of Criminal Procedure.

1) Security Police Act

The most important law regarding the use of facial images by the police is the Security Police Act. This law provides the grounds for obtaining facial images from persons and storing, searching and deleting those images during criminal investigations. The regulation regarding the deletion of images partly comes from the Data Protection Law.

2) Code of Criminal Procedure

The collection of crime scene related facial images is regulated by the Code of Criminal Procedure, but the processing of those images in the database is regulated by the Security Police Act.

3) Federal Law on Foreigners and Asylum (BFA-VG)

BFA-VG stipulates the details about data collection and processing in the Central register of foreigners holding information for non-citizens of Austria.

4) Regulations concerning the use of civil databases

The police are allowed to ask for an image of a person of interest from other databases, including civil databases. However, FR searches with crime scene related images (i.e. uncontrolled images) are not allowed within civil databases. The prohibition is stated in an explanatory memorandum to the Security Police Act.

2. Civil databases

There are four major civil databases in Austria that contain facial images:

- Central register of foreigners (*Zentrales Fremdenregister*);
- Identity documents register (*Identitätsdokumentenregister*);
- Social security register;
- Driver’s licence database (*Führerscheinregister*).

FR searches for criminal investigation purposes are not permitted in the Identity documents register, the Social security register nor in the Driver’s licence database. Nevertheless, according to the Penalty Law, the police may request images from these databases. Not only legally, but also technically, it is not possible to perform FR searches in these three registers.

1) Central register of foreigners

The Central register of foreigners is considered to be a civil database. Nevertheless, legally it is permissible to perform FR searches in this register during criminal investigations and, for this reason, the register has been described above in Section 1.3.2.

2) Identity documents register

The Identity documents register contains information collected during the application process for ID-cards and passports. In Austria, neither a passport nor an ID-card is a mandatory document for Austrian citizens. In addition, since the beginning of 2020, the Identity documents register also contains data and photographs of persons who are obliged to register a facial image for the issuing of a social security card (e-card). The obligation applies to persons older than 14 years of age who do not already have a photograph in the Identity documents register, the Driver's licence database or the Central register of foreigners.

Several types of passport are issued (e.g. regular Austrian passport, service passport for persons working in certain government positions, diplomatic passport, and emergency passport for those who have lost a previously issued passport). If a person does not have a passport, ID-card or a driver's licence, during the issuing process of a document, their identity can be proved with a birth certificate and a witness testimony (e.g. the main use case is the first application for a children's passport). The witness himself has to present a passport or an ID-card to the authority. In order to apply for an identity document, an individual must appear in person to a relevant authority (online application is not allowed). For data protection purposes, it is forbidden to have a unique identifier of a person in Austria that could be used in all databases. To match a person in different registers a special cryptographic procedure is used.

The Federal Ministry of Interior is the owner of the database, but the data is owned by the authority that collects the data. Approximately 130 local authorities in Austria and 100 authorities abroad (embassies, consulates) collect the data for issuing travel documents. Approximately 6 million Austrians have either a passport or an ID-card and therefore, their data is entered into the Identity documents register.

A frontal view facial image of an applicant of a passport or an ID-card is collected and entered into the register. Usually, applicants of identity documents provide a photograph in a paper format taken by a professional photographer and the photograph is scanned by the document officer. However, the photograph can also be captured by the document officer.

If the image of a person is enrolled several times, all the images are retained in the database until the legal point for deletion is reached. The image is retained in the database for six years after the expiry of a document and thereafter it must be deleted from the registry. There is a regulation in place describing the quality requirement for the photographs. Image quality is checked during the interview with the document applicant. Document officers are all trained to ensure that good quality images are entered into the database. Procedures for capturing photographs and checking the image quality are described in the training materials for the document officers.

In addition to images, biographic data, signatures and fingerprints are also collected. The biographic data (name, date and place of birth etc.) entered into the database is the same for passports and ID-cards. Fingerprints are collected for the purpose of including them in the biometric passport and must be deleted from the register in the 2–4-month period after the document is issued. At the present time, fingerprints are not stored within Austrian ID-cards, but legal changes to the ID-card policy are currently being prepared.

The Identity documents register is legally regulated by the Passport Act accompanied by lower-level legislative acts.

3) Social security register

For social security purposes (health, pension and accident insurance) chip-cards (called e-cards) are used in Austria. As of January 2020, new e-cards with a photograph were issued. Facial images for the production of e-cards are taken directly from other registers (e.g. Identity documents register, Driver’s licence database). If a photo of a person is not available in those registers, the person (over 14 years of age) is obliged to register a photograph for this purpose in the Identity document register. Photographs from other registers are not transferred to the Social security register.

4) Driver’s licence database

The Driver’s licence database is owned by the Ministry for Traffic and Technology.

Belgium

1. Facial recognition in relation to criminal activity

As of February 2020, FR has not been implemented in Belgium in relation to criminal investigations. The principal reason for this is the legal restrictions that exist within the country. There is legislation in place that allows the police to use intelligent cameras for law enforcement purposes but, it is not permissible to keep track of the captured images (even for a few seconds). Thus, in general, such cameras can only be used in real-time unless specific legislation is in place to create a technical database of the images for a specific purpose. At the present time this has only been done for the images from automatic number plate recognition (ANPR) cameras in order to track vehicles. Thus, the application of FR technology is not legally viable without legislation changes.

Further legal restrictions arise because the police are only allowed to process certain categories of personal information and that does not include the faces of unknown/accidental passers-by. Thereby, even the real-time monitoring of facial images can present legal difficulties.

After the Brussels terrorist bomb attacks in March 2016, a pilot project using FR was started at Brussels Airport but, concerns were expressed by the Belgian Data Protection Authority (GBA) about the legality of these activities and this led to the work being stopped. Following this, a working group was set up internally by the police to assess their requirements for processing biometric data (broader than just FR) with the intention to explore what is possible within the current legal framework and to make proposals for changes to the law.

Thus, there are currently no explicit plans in Belgium to introduce FR technology for law enforcement purposes.

There is a general national database in Belgium that contains data for suspects (photographs, fingerprints and individual descriptions) in the event of a judicial offence.

Explicitly, with a judicial mandate, it is permissible for facial images captured in Belgium for other purposes (e.g. applications for official documents such as ID cards, passports, driver's licences) to be used in criminal investigations.

Bulgaria

1. Facial recognition in relation to criminal activity

As of November 2019, FR has not been implemented in Bulgaria in relation to criminal investigations. This is due to a lack of finance and a lack of relevant legislation. However, should FR be implmented in the future, the Ministry of Interior would be responsible for the work.

Facial images that are collected during criminal investigations are entered into the Criminal Record Police System. The owner of that system is the Ministry of Interior, General Police Directorate. Facial images (frontal, profile and semiprofile) are taken at police stations together with fingerprints. While facial images are stored in the Criminal Record Police System, fingerprints and DNA samples are sent to the Research Institute of Forensic Science who are the custodian of the respective databases. There are no plans about making the system available for FR purposes.

Currently, only 1:1 comparisons of facial images are performed by the Research Institute of Forensic Science. For 1:1 comparisons, as a rule, images of known persons are retrieved from the Bulgarian Identity Documents Database. In some cases, images can be taken from the Criminal Record Police System.

2. Civil databases

There is one major civil database in Bulgaria that contain facial images known as the Database of the Bulgarian Identity Documents. The owner of the database is the Ministry of Interior. The database includes images for:

- Passports;
- ID cards;
- Driving licences.

Since 2000, all images stored in the database are in a digital format and no photos are accepted on paper. Images are captured and enrolled automatically in a kiosk.

Facial images are not linked to other biometrics. Fingerprints that are taken for biometric passports, are deleted after the document has been issued.

Croatia

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of December 2020, FR has not been implemented in Croatia in relation to criminal investigations. However, FR implementation is underway and it is expected to become operational in the first half of 2021.

The FR search facility will be available on two databases:

- ABIS, which is used for storing data from suspects and offenders;
- Image repository of civil documents that stores the photographs of applicants associated with the Registry of ID cards, the Registry of travel documents and the Registry of driver's licences.

Both FR systems are owned by the Ministry of Interior and it is permissible for them to be used in relation to criminal investigations for the purposes stipulated in the Biometric Data Processing Law. The Biometric Data Processing Law was adopted and came into force on 4 January 2020. In addition, a regulation implementing the law known as the Ordinance on Biometric Data Processing came into force on 17 November 2020.

Currently, only manual 1:1 facial image comparisons are performed by the forensic experts at the Forensic Science Centre "Ivan Vučetić" (FSC). The results from these comparisons can be applied as evidence in the courts.

1.2. Organisations involved

The Ministry of Interior is the owner of both ABIS and the image repository of civil documents where FR is being implemented and is also the owner of the respective data. The implementation of FR in ABIS is the responsibility of FSC under the Ministry of Interior, whilst the implementation of FR in the civil system is the responsibility of the Criminal Police Directorate of the Ministry of Interior.

1.3. Databases that contain facial images and are permitted to be used for facial recognition in relation to criminal activity

1.3.1. ABIS

ABIS has been established using data from suspects and offenders that used to be stored in the Fingerprint database. As of January 2020, approximately 220 000 individuals are registered in the database. While the Fingerprint database was used primarily for the purpose of storing and searching fingerprints, the facial modality was added with the purchase of the ABIS system.

ABIS is owned by the Ministry of Interior of Croatia and the custodian of the system is FSC. ABIS runs on software from Idemia.

Since 2010, individuals providing fingerprints have also been photographed. For databasing purposes, the fingerprints have been collected on a special fingerprint card and the photographs of the individual have also been included. Thus, most of the facial images sent to FSC are in a paper format, whereas the original copies of these images are stored in a digital format in the police departments across the country where the photographs were taken. The process of populating ABIS with facial images that are digitally available within police departments across the country, is currently underway.

Facial images are taken as three views and will be enrolled into ABIS in JPEG format:

- Frontal view facial image;
- Right profile view facial image;
- Left half-profile view facial image.

Photographs are captured using a standard setup that involves a digital camera and special lighting. All the cameras that are in use have similar technical specifications. The quality of an image is checked by the person capturing the image (i.e. police officers and criminalistic technicians at police stations). Facial images are entered into ABIS by forensic technicians at FSC. However, in the future, when livescan systems are acquired, photographs will be automatically enrolled into the database by criminalistic technicians at police stations.

Facial images will be retained in ABIS for a time period depending on the type of crime involved, ranging from 10 to 20 years. After the retention time expires, images are removed according to the law.

Alongside images, biographic data such as name, surname, name of parents, date and place of birth, personal identification number, citizenship, residence address, nicknames and description of a person (e.g. height, shape of face, nose and eyes, hair colour) will be stored in ABIS for each individual.

In order to avoid double entries for the same individual, biographic data is checked using an identity document (e.g. ID card). If there is no identity document available, witnesses may be asked to ascertain the identity of a given person. In addition, the police officer may verify the identity of the person by searching his/her fingerprints.

It has not yet been decided whether uncontrolled images will be stored in ABIS.

1.3.2. Image repository of civil documents

A common image repository of civil documents is used for storing the facial images that are obtained during the issuing of ID cards, passports and driver's licences. Software for the repository has been developed in-house by the Ministry of Interior. The image repository is connected to the following civil databases:

- Registry of ID cards;
- Registry of travel documents;
- Registry of driver's licences.

Altogether, the image repository of civil documents contains around 18 million images from approximately 5.7 million people. It is permissible to use these images, collected during document applications, for FR searches in criminal investigations and in the search for missing persons.

The three above-named registries are described in more detail in Section 2.

1.4. Facial recognition searches

FR searches in Croatia in relation to criminal investigations are permissible in two separate systems where FR functionality is being implemented – in ABIS as described in Section 1.3.1. and in the image repository of civil documents as described in 1.3.2. The search engine in both systems is IntellQ from a Croatian company IntellByte. Only frontal images will be searched.
Forensic experts of FSC, who started as fingerprint experts, have been trained in facial image comparison and will start performing FR searches. At the present time, there are three forensic facial experts at FSC.

According to the current plans, FR searches in both systems will be performed by the forensic experts of FSC. Additionally, the searches in the image repository of civil documents can also be made by police officers.

The results of the searches that are performed by the police officers can be used for operational and intelligence purposes, but not for identification. The results of the FR searches conducted by the forensic experts at FSC can be used for identification, but only if the search is followed by a manual 1:1 facial image comparison. Only the results of 1:1 comparisons can be applied as evidence in the courts.

1.5. Quality assurance of ABIS

The criminalistic technicians of the Croatian Police are trained to capture facial images. Photographs are taken in accordance with an internal guideline known as a ´Rulebook on fingerprinting and photographing persons´.

The forensic technicians of FSC have been trained in image enrolment and the forensic experts of FSC in performing FR searches. In the future, written methods or SOPs for facial image enrolment and FR searches will be developed.

In addition, it is planned to train more forensic experts in 1:1 facial image comparison as well as in FRcognition searches.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The Biometric Data Processing Law (https://zakon.hr/z/2431/Zakon-o-obradi-biometrijskih-podataka), which came into force on 4 January 2020 stipulates that FR searches are allowed to be performed for the following reasons:

- For criminal investigation purposes;
- For searching of missing persons;
- For prevention of the misuse of identities;
- For establishing the identity of deceased persons;
- For checking existence of previous records on persons who apply for international protection;
- For checking existence of previous records on third country nationals or stateless persons who:
    - Reside in Croatia illegally;
    - Apply for visa;
    - Are crossing the state border;
    - Are not admitted to enter Croatia.

2. Civil databases

The main civil databases in Croatia that contain facial images are:

- Registry of ID cards;
- Registry of travel documents;
- Registry of driver’s licences.

The Registry of ID cards is the largest database with facial images. The ID card is a mandatory document for every Croatian citizen residing in Croatia from the age of 18 years. As of December 2019, there were more than 3.8 million valid ID cards issued to Croatian citizens living in Croatia and more than 178 000 residing abroad. Approximately 600 000 new ID cards are issued each year, 40 000–50 000 of these to Croatian citizens living abroad. ID cards are valid for 5 years.

The Registry of travel documents is the second largest database containing facial images. In 2019, approximately 175 000 new passports were issued, out of which more than 123 000 were issued in Croatia and more than 52 000 issued in Croatian consulates abroad. Passports are valid for 10 years.

The Registry of driver's licences contains images of people that have applied for a driver's licence.

The owner and custodian of the Registry of ID cards, the Registry of travel documents and the Registry of driver's licences (hereinafter Registries) is the Ministry of Interior. The facial images associated with these Registries are stored in one image repository that is connected to the Registries. Thus, all images taken of a person for various documents can be accessed together.

For document applications, photographs (frontal view) can be submitted only in a paper format. Digital images are not accepted. Images are taken by professional photographers according to the standards published on the website of the Ministry of Interior.

All the above-named documents can be applied for at the offices of the Ministry of Interior. This is currently the only possibility when applying for an ID card. Applications for passports can also be submitted at the diplomatic and consular offices of Croatia abroad. Additionally, applications for passports and driver's licences can be submitted electronically via an e-Citizen system, but in this case, a photograph must already be stored in the Registry for a previously issued and still valid document, that is not older than 5 years and on which the appearance of the person has not changed substantially. For passports, previously stored fingerprints are also required.

Officers at the administrative services units in police administrations (regional level) and police stations (local level) compare the look of the person with the submitted photograph and previously stored photographs before entry into the Registry. The entry of photographs is performed by the officers of the same administrative services units and police stations for all three Registries. For entering images into the Registry, the paper photographs are scanned and thereby digitised. The officers performing this task are trained to use the scanning equipment and to introduce the images into the Registries.

Images are retained in the Registries indefinitely. The number of images in the Registries per person is not limited.

The Registries are linked to the Registry of residence, through which authorized officers can access the following data: name, date and place of birth, names of parents, residence address for persons residing in Croatia, personal identification number, gender, unique registries number of the citizen, nationality, level of education and profession.

The fingerprints associated with ID cards and passport applicants are also stored in a database.

Czech Republic

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of February 2020, FR has not been implemented in the Czech Republic in relation to criminal investigations. However, preparations for its implementation are underway. This is the responsibility of the Police of Czech Republic – the Police Presidium and the Institute of Criminalistics.

In 2019, the Law on Police of Czech Republic (Act No. 273/2008 Sb.) was changed, authorizing the Police of Czech Republic to use FR technology and allowing images from the Population register of natural persons to be used for FR searches, e.g. for the solving of crimes, the identification of persons and the identification of dead bodies.

At the present time, a new multimodal biometric system for fingerprints and facial images is being developed with a procurement process underway to acquire the necessary software for the inclusion of FR search functionality. The system being developed is known as the Central Biometric Information System (CBIS) and it is expected to become fully operational in 2021.

CBIS will be populated with images from the Registry of suspected, accused and/or convicted persons (FODAGEN) and it will be linked with the Population register of natural persons (Population register). Images in the Population register will be accessible via CBIS in accord with the change in the law, permitting such images to be used for FR searches in criminal investigations.

1.2. Organisations involved

The Police of Czech Republic is responsible for the implementation of FR in the investigation of crime.

1.3. FODAGEN

FODAGEN is a database used for storing fingerprints and photographs. It is owned by the Police of Czech Republic and operates on software developed in-house. As of February 2020, it contains between 200 000 and 300 000 records of suspected, accused and/or convicted persons.

The stored photographs include facial images (frontal view, right side view and left half-side view), as well as a full body image and images of special marks and/or tattoos. New images are added only when the appearance of the person has changed (e.g. due to aging). There are no limits for the number of images that can be stored per person. Images in the database are taken by police officers at police stations in general custody rooms, police office rooms or specially fitted image capturing stations. Digital cameras are used for the image capturing.

In addition to biometric data, the following metadata are stored in FODAGEN: name, date of birth, place of residence, gender, personal identification number, crime a person is accused of (convicted for), history of previous criminal records, information as to whether fingerprints and DNA have been taken and stored in relevant databases.

Currently, only administrative data is checked in order to avoid any double enrolment of identities, i.e. a situation of having more than one identity for a given individual.

The data storage time period depends on the type of crime committed, ranging from 5 to 30 years. If a person is acquitted, data will be deleted according to the court order. A person can also ask for a deletion of his/her data. In such a case, the police or the court will decide whether the data can be deleted.

There are no uncontrolled images stored in the FODAGEN database, but there are current discussions as to whether uncontrolled images should be included to CBIS.

1.4. Facial recognition searches

FR search functionality is not available in FODAGEN, but will be available in CBIS. The installation of a central workstation is planned for this purpose, to process search queries from the police and to connect it with other information systems in the Czech Republic and Europe. Also, data in the Population register will be accessible for FR search purposes.

1.5. Quality assurance

The data format of the facial images in FODAGEN are regulated by internal quality requirements. These requirements are for the most part in accordance with the ICAO standard. Technical parameters for digital images are as follows:

- Format – JPEG and JPEF/JFIF;
- Size – maximum 90 kB, minimum 50 kB;
- Colour depth of 24 bits (in RGB mode).

There are internal regulations for personnel capturing facial images and training is provided during special courses for police officers performing this task.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The use of facial images in relation to criminal activity is regulated by the Law on Police of Czech Republic (www.zakonyprolidi.cz/cs/2008-273/zneni-20190424).

The Population register, which can be accessed during criminal investigations, is regulated by the following legal acts:

- Act No. 328/1999 Sb. “Act on Identity Cards”;
- Act No. 133/2000 Sb. “Inhabitants records act”;
- Act No. 111/2009 Sb. “Law on basic registers”.

These acts enable the creation of the Population registry and regulate how it is managed and how information is included.

2. Civil databases

There are four major civil databases in the Czech Republic:

- Population register;
- Passport database;
- Driving licence database;
- Visa database.

The Population register is owned by the Ministry of Internal Affairs and contains 11 million records on the inhabitants of the Czech Republic and persons with long-term visa or long-term residency permits. It runs on a population evidence information software system called AISEO. Facial images that are taken in the process of issuing ID cards (a mandatory document for every Czech citizen and every person above 15 years of age permanently living in the Czech

Republic) are stored in the Population register. Images (frontal view) are taken by local authorities at several offices around the country in specially fitted image capturing stations or rooms by digital cameras according to the ICAO standard. A public notice 400/2011 Sb., on standards for ID documents including facial images for ID documents is available at: www.zakonyprolidi.cz/cs/2011-400. No paper images are accepted for ID card applications. This requirement has been in force for the last 7 years. With it being compulsory for every Czech citizen to have an ID card, at least one digital image per person should be in the database. There are no limits for the number of images that can be stored per person.

Metadata stored in the Population register alongside the facial images are name, date and place of birth, place of residence, gender, personal identification number, marital status, address, prohibition of stay, day of death etc. No other biometric data (e.g. fingerprints) are taken for issuing ID cards.

Data on a person in the Population register is automatically deleted 15 years after the death of the given person or 15 years after a court has issued a declaration of a death.

Facial images are also taken for other document applications: the issue of passports, driving licences and visas. However, images in passport and visa applications are used only for the issuing of the documents and are not stored. Images in driving licence applications are stored in a relevant database owned by the Ministry of Transport.

Data in all civil databases can be checked against the Population register.

The Law on Police of Czech Republic adopted in 2019, theoretically, permits the use of images in civil databases for FR searches in criminal investigations. Nevertheless, this is not technically possible at the present time.

Cyprus

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of May 2020, automated FR has not been implemented in Cyprus in relation to criminal investigation. However, the preparation for its implementation is underway. The Photographic and Graphic Laboratory of Criminalistic Services responsible for the implementation has acquired a FR system (ISIS Faces Fire from Unidas). The implementation is expected to finish during 2021–2022.

In addition, the Criminalistic Services of Cyprus Police has a database known as ISIS Faces that contains the facial images of convicted persons and there are plans to use it for FR searches in criminal investigations.

At the present time, only manual 1:1 facial image comparisons are performed by facial comparison experts of the Photographic and Graphic Laboratory of Criminalistic Services. The results of these comparisons can be used as evidence in court.

1.2. ISIS Faces

The owner and custodian of the ISIS Faces database is the Criminalistic Services of Cyprus Police. The database runs on software of the same name produced by the company Unidas.

At the present time, only the database storage of facial images for convicted persons is permissible according to the Cypriotic legislation. As of May 2020, about 2000 individuals have facial images stored in ISIS Faces. In the future, when an amendment to the law has been adopted, the images of unconvicted suspects will also be stored. This will increase the size of ISIS Faces by the addition of images from around 45 000 individuals.

Facial images are taken by police photographers in 6 Divisions of the Criminal Investigation Department of Cyprus Police across the country. Digital single lens reflex cameras are used for image capture. The requirements for image capture include a one colour background (grey), the camera placed 3 meters away from the person being photographed etc. Images that are entered into ISIS Faces are of low compression JPEG format with a resolution of 12 megapixels.

Photographs stored in the database are not limited to frontal views with individuals also portrayed at different angles such as side views and 45-degree views. The database allows for the storage of a large number of photographs per individual (up to 200). The facial images are entered in the database by the personnel of the Photographic and Graphic Laboratory of Criminalistic Services.

In addition to the facial images, various metadata for the person are entered into the database (e.g. name, surname). With new entries in the database, measures are taken by a responsible employee of the Criminalistic Services of Cyprus Police, to prevent double enrolment arising from aliases.

The facial data stored in the database is linked to fingerprint data. A separate AFIS-system generates a number associated with the individual and this number is also stored in the ISIS Faces database.

The images in the ISIS Face database are retained in line with the time periods as stipulated in the Cypriotic legislation. The retention times will vary depending on the criminal activity associated with the respective entries.

No uncontrolled images are stored in the ISIS Faces database.

Denmark

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of September 2019, FR has not been implemented in Denmark and there are no specific plans for the implementation of FR. However, relevant discussions around this topic have taken place at a national level and there is an interest in implementing the technology. Nevertheless, no open debate on the potential use of FR has been finalised and no conceptual decisions on the implementation have been made. Furthermore, there are no legal regulations in place that would enable FR to be used in criminal investigations.

In addition, there are no decisions yet as to which organisation will be responsible for the implementation of FR for criminal investigation purposes. It is suggested that it could be the responsibility of either the National Forensic Centre or the National Centre of Investigation of the Danish National Police.

Only one database related to the investigation of crime, containing facial images, is in existence (National Photo Database of the Danish National Police). In theory, this could be considered for FR but, there are no current plans for it to be used for this purpose at this time.

Currently, the investigation of crime is done solely by manual 1:1 facial image comparison. This work is performed by the Danish National Police. It is not permitted to use facial images that are captured for civil use (i.e. from various document applications) for this purpose.

1.2. National Photo Database

The National Photo Database contains facial images of individuals that are suspected of crimes where conviction could lead to imprisonment for more than 1.5 years. The number of individuals registered in the database is approximately 250 000. The database is owned by the Danish Police. The software that is used for database management is MS SQL Server 2017 Management Studio.

The capturing of images for the National Photo Database is performed by police officers at police stations in special rooms with special camera and light setups. There is no specific training for image capturing. Instead, police officers who take images, are instructed on how to use a standard setup, how to position a person who is being photographed etc. In addition, there are written instructions in the system that act as guidance for the procedures.

For each person, front view, right side and left side images are taken and entered into the database. The file format for images is JPEG and images are compressed by using .NET framework's built-in scaling logic. Image resolution for photos varies depending on the camera: from 4272 x 2848 pixels to 6000 x 4000 pixels.

Biographic data that are entered into the National Photo Database include the mandatory information such as full name, gender, date of birth, social security number. In addition, voluntary data about physical characteristics can also be included (e.g. eye colour, hair colour, body build, description of tattoos and other special features).

Each image in the database is linked to the registration number of the criminal case through which it was obtained. Using the case management system, it is possible to use the same registration number to access all relevant case information, including whether fingerprints and DNA have been collected.

As a rule, images are kept in the database for 12 years before being deleted. Images may also be deleted sooner depending on the sentence for a particular crime committed.

No uncontrolled images are kept in this database.

The legislative act that regulates the use of biometric data, including the use of facial images by law enforcement agencies is the Danish Administration of Justice Act (*Retsplejeloven*).

2. Civil database – CARL2 database

Central Address Register Solution 2 (CARL2) is one of the civil databases in Denmark. The CARL2 database is owned by the Ministry of Immigration and Integration. It is used for processing the various applications from aliens (third country nationals and EU citizens) when applying for asylum, visa or residence for family reunification purposes, or to work or study in Denmark. Facial images that are entered into the CARL2 database are taken solely from third country nationals. Facial images are accepted only in a digital format.

Data that are entered into the CARL2 database:

- Full name;
- Nationality;
- Date of birth;
- Unique alien's identification number;
- National ID number (if a person gets a residence permit in Denmark);
- Residence address;
- Signature;
- Fingerprints – tenprints for visa applications (from 1 July 2017) and two prints for other applications (according to EU legislation, fingerprints for other applications that were taken before 1 July 2017, were kept temporarily until the residence card was issued, since the named date these fingerprints are kept for up to 10 years).

At the beginning of September 2019, there were more than 3 million registrations in the CARL2 database. More than one registration per individual may exist. However, the number of registrations of individuals whose facial image has been entered into the database is notably smaller.

During the registration of a person whose data is already in the database, previous photographs are not replaced by the latest one, instead all photographs from different registrations are retained. With reference to fingerprints, at the current time, several sets of fingerprints are retained. However, the introduction of a solution to identify duplicated fingerprints is planned to be in place by the end of 2021 or the beginning of 2022 and, after that, only the latest set of prints will be stored.

Frontal view images are captured using special capturing stations by the following authorities:

- Danish Immigration Service – images of asylum applicants (from 1 August 2020, but previously by the Danish National Police before this date) and family reunification applicants;
- Danish Agency for International Recruitment and Integration – images for student permits, work permits and au pair permits;
- Ministry of Foreign Affairs – images of visa applicants and residence applicants.

There are written instructions and on-the-job training is provided to personnel on how to capture facial images with the capturing stations. The facial images captured and enrolled into the CARL2 database follow the quality requirements described in the EU uniform standard for issuing of residence cards to third country nationals (asylum/residence permits) and the VIS standard for visa applicants.

Facial images are kept in the database for 10 years where the person applies for and receives a residence permit. If the person does not receive a permit, then the data can be kept for up to 20 years.

Legally, the use of the CARL2 database is in line with the general legislation on databases in Denmark and with the European GDPR. In addition, regulations stipulated in the Aliens Law are followed.

With the provision of assistance from the Danish immigration authorities, the Danish National ID-Centre’s biometric team of nine persons performs manual 1:1 facial image comparisons for identification purposes, as necessary. At this time, FR searches in the CARL2 database are not performed but, it is intended that FR technology for deduplication purposes will be implemented in the future.

Nevertheless, there are no plans to make the CARL2 database available for FR searches in crime investigation.

Estonia

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of October 2020, FR has not been implemented in Estonia. However, preparations to implement FR for the investigation of crime are underway. Technically, FR functionality will be available on a multimodal ABIS. The ABIS, procured in 2020, will be used as a central biometric repository for storing fingerprint and facial image data collected by the state during both criminal and civil proceedings. The criminal and civil datasets will be logically separated in ABIS and are referred to as the criminal-ABIS and the civil-ABIS.

The collection of facial images for the criminal-ABIS will start once amendments to the law have been implemented and a technical solution is in place. The criminal-ABIS will not be populated with images previously collected for criminal investigation purposes. Final decisions have yet to been taken but, most probably, facial images will be captured from suspects, accused and convicted persons for the prevention and detection of criminal offences. Typically, they will be captured alongside fingerprints and DNA. The facial data collection and FR are expected to launch by the beginning of 2022.

The civil-ABIS will be populated with facial images from existing databases that are used in various document procedures. The Estonian legal framework currently allows the civil fingerprint database to be accessed for solving the most serious crimes, and the same principle will probably be applied for facial images. Therefore, it is likely that at least some of the facial images that are collected for civil purposes will be available for FR searches in criminal investigations.

At this time, only manual 1:1 facial image comparisons are performed by face experts at the Estonian Forensic Science Institute.

1.2. Organisations involved

The multimodal ABIS used for storing biometric data and performing the searches, is owned by the Ministry of Interior. The ABIS is maintained by the IT and Development Centre of the Ministry of Interior (SMIT – *Siseministeeriumi Infotehnoloogia ja Arenduskeskus*).

The main users of the criminal-ABIS will be:

- Estonian Police and Border Guard Board (PPA – *Politsei ja Piirivalveamet*) under the Ministry of Interior, and
- Estonian Forensic Science Institute (EKEI – *Eesti Kohtuekspertiisi Instituut*) under the Ministry of Justice.

The exact roles of these two authorities will be decided in the near future. However, it is already known that the majority of facial images from individuals will be captured during pre-trial investigations by the police officers of the Estonian Police and Border Guard Board.

1.3. ABIS

In 2017, the Government of Estonia decided to establish a multimodal ABIS. It is intended that ABIS will be used as a centralized database for storing all the biometric data collected by the state. In the beginning, ABIS will include two biometric modalities – fingerprints and facial data. Nevertheless, the possibility of adding other modalities to the database in the future is being considered.

The technical solution for the ABIS system, as provided by Idemia, is designed to be a multi-biometric identification system for criminal investigations, a biometric recognition system for civil applications and a multibiometric search service.

ABIS will contain biometric information from both criminal and civil proceedings. These two datasets, criminal biometry and civil biometry, are logically separated from each other in ABIS. The criminal part of ABIS (i.e. criminal-ABIS) is expected to be operational in March 2021 and, in the first phase, will only contain fingerprints transferred from the previous criminal-AFIS that has been used in the past. The facial modality of the criminal-ABIS is expected to be functional at the beginning of 2022. The civil part of ABIS (i.e. civil-ABIS) is expected to be introduced during 2022.

Currently, in parallel to the technical preparations, amendments to the law are being prepared. It is highly likely that photographs will be taken from the same groups of people whose fingerprints and DNA are collected during criminal and misdemeanour proceedings. In short:

- During criminal proceedings, it is obligatory to collect and enter information into biometric databases, for persons suspected, accused, or convicted of crimes for which there is a potential imprisonment punishment of at least two years.
- If the potential imprisonment punishment in criminal proceedings is between one and two years, the investigation authorities are allowed to collect the biometry and enter the data into databases.
- During misdemeanour proceedings, biometry can be collected and entered into the databases in certain cases related to narcotic substances.

Estonia does not have digital facial data that can be moved into the criminal-ABIS. Thus, the collection of facial images will start from the moment when the facial modality in ABIS is implemented for criminal investigation purposes and the law amendments are adopted. It is planned that the following image types will be captured and entered into ABIS:

- Front view facial image;
- Side view facial image;
- Half-side view facial image;
- Full body image;
- Special marks and tattoos.

The collection of facial images for dead bodies of unknown identity and for missing persons are also being considered.

It is most likely that, in most instances, all biometric data (fingerprints, facial images and DNA) will be collected together during the same process.

It is highly likely that facial data will be retained within ABIS using the same rules that are currently applied for fingerprints and DNA. Thus, controlled images would be stored in ABIS for 40 years, after which they will be archived for 35 years. If a person is acquitted, the relevant biometric data must be deleted from the databases.

In the future, it is planned to use ABIS only as a repository for the biometric information and store all other personal and case data outside ABIS in dedicated databases. However, at the beginning, the criminal-ABIS will also be used to store some basic biographic information (e.g. name, personal ID-code etc.) and case related data (e.g. case number). This will remain in place until the corresponding IT system development work has been completed.

It has not yet been decided whether uncontrolled facial images will be stored in the criminal-ABIS.

1.4. Facial recognition searches

At present, no final decisions have been made as to who is going to conduct the FR searches and how the searches will be performed. Similarly, no decisions have been taken as to whether or not live FR searches will be conducted.

1.5. Quality assurance for the images in the criminal-ABIS

ICAO based image quality standards have been built into ABIS and the system automatically follows these standards for the verification of an image when it is being enrolled into the system. All other quality related topics (starting from SOPs and ending with the training of staff) have not yet been developed to the point where there is enough information to be reported.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

As of October 2020, amendments to the law to establish the use of the multimodal ABIS for criminal and civil use are still in preparation. These amendments must be approved by the Parliament before the launch of the criminal-ABIS, which is planned for March 2021. It is reasonable to assume that legal regulations stipulating the collection, storage and use of facial images will be the same as those currently being used for fingerprints and DNA.

The following is a list of the most important laws regulating the collection and use of biometric data (currently fingerprints and DNA, but facial images will likely to be added soon):

- Code of Criminal Procedure;
- Code of Misdemeanour Procedure;
- Imprisonment Act;
- Forensic Examination Act.

These laws can be found on the *Riigi Teataja* website: www.riigiteataja.ee/en/search.

A short summary of the most important regulations in the laws listed above:

- Section 1, § 99^1 Code of Criminal Procedure – biometric data (currently DNA and fingerprints, facial images presumably in the future) can be collected for detection and prevention of crimes from a suspect, accused or convicted person if imprisonment for the crime committed is two or more years.
- Section 2, § 99^1 Code of Criminal Procedure – biometric data (currently DNA and fingerprints, facial images presumably in the future) may be collected for detection and prevention of crimes from a suspect, accused or convicted person if imprisonment for the crime committed is at least one year but less than two years.
- Section 4, § 99^1 Code of Criminal Procedure – the biometric data (currently DNA and fingerprints, facial images presumably in the future) obtained under the Sections 1 and 2 of § 99^1 Code of Criminal Procedure shall be entered in the respective state registers.
- § 31^1 Code of Misdemeanour Procedure – biometric data (currently DNA and fingerprints, facial images presumably in the future) may be collected for detection and prevention of crimes from a person suspected of a crime related to certain narcotic substances. Data obtained shall be entered to the respective state registers.
- § 18 Imprisonment Act – biometric data (currently DNA and fingerprints, facial images presumably in the future), if not collected previously in the course of criminal proceedings, shall be collected for detection and prevention of crimes as well as for identification purposes from a person who is received into a prison for serving a sentence. Data obtained shall be entered to the respective state registers.
- Section 1, § 9^9 Forensic Examination Act – biometric data (currently DNA and fingerprints, facial images presumably in the future) shall be stored for the term of 40

years as of the entry of the data in the respective databases, unless otherwise provided by law. After expiry of the specified term, the data shall be closed and archived.
- Section 2, § 9[9] Forensic Examination Act – upon acquittal of a person, termination of criminal proceedings or termination of misdemeanour proceedings, biometric data (currently DNA and fingerprints, facial images presumably in the future) shall be deleted within 14 days.

1.7. Other databases and registers related to criminal activity that are not going to be used for facial recognition in the near future

The following two infosystems are described in this section:
- Information system POLIS – police case data management system;
- Prisoners' register or KIR in short – database of prisoners, detained persons, persons in custody and probationers.

1) POLIS

Infosystem POLIS is used for storing and processing data collected during different procedures carried out by the police. Among other information, POLIS contains photographs related to persons, vehicles and cases. Photographs of people can be from both, known and unknown individuals. In addition, POLIS contains images of missing persons and wanted persons. Photographs of people can be taken by the police or by some other person or they can be obtained from any other sources (e.g. social media) or from other state-owned databases. The number of photographs in POLIS is estimated to be around 100 000.

The photographs of people in POLIS cannot be automatically used for FR purposes due to the wide variability and unequal quality of the images. However, in the future, some of the facial images in POLIS will probably be searched against ABIS, as uncontrolled images.

No other biometric data is entered into POLIS.

The owner of POLIS is the Police and Border Guard Board. The data in POLIS are used by different law enforcement authorities, Road Administration and the Emergency Response Centre.

POLIS is legally regulated by the Police and Border Guard Act and by the Statutes of the Police Database.

2) KIR

KIR holds records for prisoners, detained persons, persons in custody and probationers. Photographs are taken of prisoners, detained persons and persons in custody (not probationers). The number of active records in KIR, that include photographs, is around 2500. The following images are captured and entered into KIR, when an individual arrives in a prison or in a detention centre:
- Frontal view facial image;
- Side view facial image;
- Images of special marks and tattoos.

The person may be photographed several times, as necessary (e.g. when his/her appearance has changed or when he/she is released from the prison). Therefore, several sets of photographs can be included for a given person. There are agreements in place regarding the procedure for taking these photographs, but there are no written instructions available at this time.

In addition to the photographs, DNA and fingerprints are also collected but these are not stored in KIR (neither DNA profiles nor fingerprints).

It can be assumed, that KIR will be linked to ABIS in the future and thereafter the fingerprints and facial images that have been collected will be available to ABIS for FR searches during criminal investigations. However, this is not planned to happen in the next few years.

The owner of KIR is the Ministry of Justice. The data in KIR are entered by the prisons and the police and are used by different law enforcement authorities.

KIR is legally regulated by the Imprisonment Act and by the Statutes of Prisoners, Detainees, Arrestees and Probationers Database.

2. Civil databases

The list of civil databases containing biometric data, including facial images, is as follows:

- Identity documents database (ITDAK) – this database is used for issuing identity documents (identity cards, passports and other types of travel document etc.);
- Register of residence permits and work permits (ETR);
- Database of persons who have acquired or lost Estonian citizenship, or to whom Estonian citizenship has been restored (KODAK);
- Database of registering prohibitions on entry (SKEELD);
- Database of registration of short-term employment in Estonia (LTR);
- Database of aliens who are staying or have stayed in Estonia illegally (ILLEGAAL2);
- Register of granting international protection (RAKS);
- Visa register;
- Motor register – this register is used for maintaining records on different type of vehicles and different documents certifying the right of an individual to drive. Facial images collected during the issue of driver's licences are stored in the Motor register. Images for this purpose are taken either at kiosks at the offices of Road Administration or from previously issued identity documents.

All the databases listed above will be linked with the civil-ABIS in the future and ABIS will function as a repository for the biometric information for all these areas. Legally, it is allowable for biometric data that was collected during different document proceedings, to be used for solving the most serious crimes. Technically, this cannot be done at the present time because the criminal and civil databases are not connected. However, in the future, it will be possible after both datasets have been transferred into ABIS.

Finland

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

On the 04.05.2020, the Criminal Intelligence Unit of the National Bureau of Investigation (NBI) [*Keskusrikospoliisi*] implemented an automated facial image search facility for the use of police officers, border guards and customs officers. The system is known by the acronym KASTU (*Kasvo Tunnistus* – in Eng. face recognition). The KASTU system does not have a dedicated facial image database, rather it accesses mugshot images in a database called the Registered Persons Identifying Features database (*Rekisteröidyn Tuntomerkit* – RETU), which is a section of the National Criminal Database, and images in the Aliens database. As part of the development of the KASTU system, RETU has been converted to allow biometric searches of the database. The RETU database contains images of persons suspected of an offence and, stored separately as part of an Aliens database, asylum seekers and aliens.

As registration on the RETU system is a pre-existing element of police registration practice, in principal any police officer can perform image enrolment. At this time 449 police officers, border guards and customs officers have completed the training course required of officers who wish to access the KASTU system. The intention is that searches of the KASTU system are not considered a specialist task, rather that it should be available to all officers who require access in relation to their duties. The reason for this approach is that the system is intended for criminal intelligence purposes only and is not considered to be suitable for official judicial proceedings. Should the need arise, 1:1 forensic comparisons of facial images are conducted by a separate unit, consisting of two experts, at the NBI Forensic Laboratory. The findings of these 1:1 comparisons can be reported in a criminal court.

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.

Current Finnish legislation states that biometric information in a database can only be used for its primary collection purpose. As an exception to this rule, certain non-criminal databases can be used for the identification of victims for example in the case of natural catastrophes and other large-scale incidents. Watch lists using an automated face recognition system are not operational in Finland at this time.

1.2. Organisations involved

The National Bureau of Investigation, Intelligence Unit is the custodian of an automated FR system. Specialist examiners at the NBI can perform searches. Searches can also be performed by law enforcement officers, border guards and customs officers.

The National Bureau of Investigation, Forensic Laboratory has a small team of facial image comparison experts who conduct 1:1 examinations of evidence supplied to them by investigators.

1.3. Databases that contain facial images and are used for facial recognition in relation to criminal activity

1.3.1. National criminal database

The Finnish Police, or other authorised organisation such as the border guard or customs agency, have the authority to enter an individual's personal identification information into the RETU section of the National criminal database for the individuals suspected of an offence.

In addition to the facial images, fingerprints and DNA, data such as full name, date of birth, national security number, aliens number (in the case of aliens), nationality, place of birth and place of residence are collected as part of the registration process.

Images taken in relation to criminal database enrolment are stored in accordance with police laws related to data protection 616/2019 and are deleted from the database when their validity has expired.

Personal identifying characteristics processed to establish identity are erased no later than ten years after the last entry concerning the person suspected of an offence. However, the data are erased no later than ten 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.

The personal identifying characteristics of a data subject who was under 15 years of age at the time of committing the offence 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.

The number of individuals registered in the National criminal database is estimated to be in the hundreds of thousands.

Enrolment into the National criminal database is performed by trained police officers, border guards and customs officers. In cases where the enrolment is performed by law enforcement officers, the procedure takes place in police station registration suits. The enrolment involves up to eight images. These are: front, left profile, right profile, front quarter profile left, front quarter profile right, back quarter profile left, back quarter profile right and full body front (sometimes with height measurement). It is common practice to store all images taken as part of crime related registration in the National criminal database. Facial images taken for enrolment into the National criminal database are captured in a standardised environment with digital cameras.

Uncontrolled images are not stored in the National criminal database.

1.3.2. Aliens database

At this time, the Aliens database is populated by asylum seekers and other non-Finnish citizens and is maintained by the Finnish Immigration Service. This is not considered to be a criminal database. However, it has a similar format to the National criminal database. Images are captured in the same way as for the National criminal database. Additional legal restrictions apply with regards to whom and for what purpose this data can be accessed (Data protection law 2: § 15).

1.4. Facial recognition searches

Due to the small population, Finnish systems such as KASTU tend to be centralized and can be accessed by more than one government agency. When a system is used by more than one department, access to the data on that system is restricted to relevant parts of the system. Not all departments have access to all parts of the system.

The KASTU system used in Finland is based on an algorithm provided by a private company. The KASTU interface was developed in Finland in a former partnership between the NBI and a private software development company. Currently, the NBI are working in cooperation with another private company in order to continue development of the KASTU system. The software used for the KASTU system is a search engine with access to the Finnish criminal- and Aliens databases that make up part of RETU.

As the KASTU system is still very new, some aspects of the FR process are still to be decided upon. There are no restrictions placed on the quality of probe images. The probe images can be cropped and adjusted for contrast before uploading to the KASTU system. It is also possible to make adjustments after uploading to the system.

However, there are guidelines in relation to the search process intended to ensure that the system will be able to provide good quality list of candidates, which includes a maximum of 200 images. As yet, no fixed criteria for establishing a match discovered with the automated face recognition system has been set.

The KASTU system is intended as a criminal intelligence tool to provide focus to police investigations. Reports provided in relation to KASTU searches are not regarded to be of evidential value in the Finnish court system. Only the NBI Forensic Laboratory has the authority to produce full statements of identification for the courts resulting from a full forensic 1:1 comparison process.

Due to the newness of the KASTU system no statistical information regarding case load and match rates is available.

1.5. Quality assurance

Recruitment into the task of FR is conducted through the normal recruitment process to law enforcement officers. No specific attributes are required.

Before a law enforcement officer can perform a search on the KASTU system he/she is required to complete a training course in the use of the automated FR and be granted official permission to use the system. This course can be completed online. In addition, officers are required to obtain permission to access the mugshot register from their department supervisor.

Additional training and permissions are required before an individual can be granted permission to search the Aliens database in accordance with the data protection law 2: § 15. Access to the Alien's database requires attendance to classroom-based training.

Law enforcement officers who have completed the KASTU training course are supplied with a brief guideline in relation to searching facial images in the system. This includes a description of the limited range of image enhancement tools available and how to go about defining acceptable levels of similarity between a searched image and suggested candidates and candidate list size. Information is also provided describing how to indicate matching facial features for the purpose of an examination report. The final section of the guideline gives an indication of the terminology to be used in the examination report such as: "Identification, probable hit", "Identification, possible hit", "Not of comparison quality", "Not identified, probably not a hit" and "Not identified, no hit".

At this time there are no proficiency tests in place for individuals operating the KASTU system.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

In the KASTU system, facial images are processed biometrically, in which case the data in question belongs to a special group of personal data. In accordance with § 15 of the Police Personal Data Act (616/2019), the police may process data belonging to special groups of personal data only if necessary and no other options are available. The KASTU system is based on the need for the police to establish the identity of an unknown individual of interest in relation to investigative and surveillance missions or to prevent or detect crime. If the identity of an unknown individual can otherwise be obtained, the KASTU system will not be used.

Personal data processed in accordance with § 6 of the Criminal Data Protection Act (1054/2018) must be appropriate and necessary for the purpose of the processing and must not exceed the purposes for which they are processed. In addition, in accordance with Chapter 1, § 2 of the Police Personal Data Act, the processing of personal data must comply with the principles of proportionality and purposefulness, in which case, the KASTU system cannot be used to investigate general/routine crime or violation. Accordingly, the National Police Board states that the KASTU system may only be used to investigate acts that could lead to imprisonment should an individual be found guilty of an offence.

The KASTU system is intended for use in relation to investigation by the police, border guards and customs officers in cases where the identity of an individual is unclear. Use of the system by the Police is in accordance with the following legislation:

- Investigative and supervisory tasks – Police Personal Data Act 616/2019, Chapter 2, § 5 and § 6.
- Persons registered on the basis of § 131 of the Aliens Act (301/2004) – Chapter 2, § 15 of the Police Personal Data Act. The information may be used where it is necessary for the prevention, detection or investigation of criminal offenses in connection with the investigation of the following types of offenses:
- Chapters 11 to 14 of the Penal Code – war crimes and crimes against humanity, treason, treason and crimes against political rights.
- Chapter 17, § 2 to § 4 of the Penal Code – riot, violent riot, § 7 state border offense, § 7c territorial violation and § 8a organisation of gross illegal entry.
- Chapter 34 of the Penal Code – § 3 aggravated destruction, § 5 aggravated endangerment of health and Chapter 34a terrorist offenses.
- Chapter 46, § 1 to § 2 – regulatory offense or aggravated regulatory offense.
- Victim identification – Chapter 2, § 15 of the Police Personal Data Act.

The above-mentioned cases must always be related to a police tasks, the case number or other similar reference of which is recorded as the basis for using the system when making a search. The access criterion is stored in the system log data to enable control of legality. For example, the identity of the person in the image included in information related to terrorist activity can be verified using the KASTU system if the content of the information is otherwise found to be accurate. By doing so, the identification allows the police to perform other registry checks related to the processing of information.

2. Civil databases

The list of civil databases that contain facial images in Finland are as follows:

- Passports register – managed by the National Police Board;
- ID-card register – managed by the National Police Board;
- Immigration service register – managed by Immigration Services;
- Driving licence register – managed by the Finnish Transport and Communications Agency [*Liikenne- ja viestintävirasto* (TRAFICOM)];
- Visa database – managed by the Ministry of Foreign Affairs.

Passport and ID-card images are mostly taken in private photography studios. However, Finnish embassies and the police station at Helsinki-Vantaa airport are also authorized to capture these images. There are currently more than 600 photographers in the country taking official passport pictures. Passport and ID-card pictures are required to conform to the ICAO 9303 standard. Photography companies are provided with online guidance as to how to take good passport and ID-card images. The passport and ID-card image process is entirely digitised in the 95% of cases where the web service is used and the 1–2% of cases where the police or an embassy services take the picture. Private individuals can in theory take and upload their own images to the passport application website. At this time only around 2–3% of applicants do so. In order to confirm the identity of the individual uploading the image, a strong authentication system is in place. The quality of these images is checked as part of the application process and when necessary images are rejected. Passport and ID-card images are enrolled into the system by trained licence administration officers. Apart from a centralized training course, there is no systematic mechanism to ensure the work quality of the officers that enrol images although, there are plans in place for a formal test to be taken on completion of the course. There are however, spot checks of the database as a whole.

Facial images from passports are deleted from the passport register three years after expiry of the passport. However, this time limit may be extended under new legislation. There is currently no limit to the number of passport pictures per person stored on the passport database. However, in practice there are seldom very many.

At this time the Finnish passport database contains certain biometric data such as fingerprints. However, the passport fingerprint database is not searchable. Only under very special circumstances can the fingerprint data held on passports be accessed.

The passports department is currently constructing a facial comparison system with the goal of preventing the registration of double identities. The intention is that this system will be operative in 2021. The system will only be used for civilian registration of passports and will not be available to the police in relation to criminal activity. However, it will be available for use in the identification of unknown deceased individuals.

France

1. Facial recognition in relation to criminal activity

1.1. Summary of the current situation

FR in France has been in use since 2013. The FR functionality is part of the criminal information system TAJ (*Traitement d'Antécédents Judiciaires)* [Criminal Case History Database] that is co-used by two police organisations in France, the National Gendarmerie and the National Police. As of October 2019, the number of facial images on TAJ was approximately 6 million out of which more than 99% were controlled images from suspects and victims (i.e. unknown dead bodies, seriously injured and missing persons) whilst the rest (approximately 6000) were uncontrolled images (e.g. photo robot sketches, surveillance images etc.). TAJ is populated with images that are captured and enrolled by both of the named organisations. FR is solely used as an investigative tool by investigators of the National Gendarmerie and the National Police who perform FR searches. Search results are used for operational purposes supporting the investigation and not as evidence in court. With the current technical infrastructure and legal landscape, it is not possible for the police to search facial images that have been recorded for civil purposes, such as applications for driving licences, passports etc. Only in very exceptional circumstances, are the police permitted to ask for such images for a 1:1 examination.

1.2. Organisations involved

The Ministry of Interior is the owner of TAJ, while TAJ is used by two police organisations in France (the National Gendarmerie and the National Police). The two named police organisations have implemented FR and are involved in the capture and enrolment of facial images as well as in performing the FR searches and manual 1:1 facial image comparisons.

1.3. TAJ

There is one searchable national facial image database for police use. This database is part of the criminal information management system known as TAJ (*Traitement d'Antécédents Judiciaires)* [Criminal Case History Database]. TAJ became operational with all its functionalities, including FR, in 2013. The use of FR in TAJ in relation to criminal investigations is legally authorised by the French data protection agency known as CNIL (*Commission Nationale Informatique et Libertés*) [National Commission on Informatics and Liberty].

In October 2019, the number of individuals that were entered in TAJ was approximately 21 million. Data from the same individual may be entered in the database several times should the person be involved in several criminal investigations. Data entries that involve the same individual are merged manually when the identity of the person has been established (e.g. by using fingerprints or DNA). However, there is currently no systematic verification of double registrations (i.e. deduplication).

Not all 21 million individuals whose data have been entered in TAJ, have photographs enrolled in this system. The number of controlled facial images in TAJ was more than 99% out of 6 million as of October 2019. Moreover, the controlled images can include multiple photographs of a given individual taken at different times and/or from different angles.

The controlled facial images that are recorded in TAJ, are from the following groups of people:

- Suspects (in the legal sense that serious and corroborated evidence makes it likely that the person may have been involved in a crime or a serious offence, either as its perpetrator or as an accomplice);

- Victims, i.e. unidentified dead bodies, seriously injured and missing persons (in October 2019, the number of photographs of dead bodies and missing persons was approximately 1000).

The types of captured image that are enrolled are face from the front, right side and left half-side, and a full body from the front. Images are taken and enrolled by forensic personnel of the National Police and investigating officers of the National Gendarmerie in respective police premises. Sometimes images can be taken at prisons. Digital cameras are used for the photography.

Alongside the facial images, the following biographic information is entered into TAJ: full name, aliases, nicknames, date and place of birth, parents' names, residence address, marital status, profession, physical description of the person such as gender, height, special marks etc., and link to offences. There are no links to other biometric data.

Data is not stored in TAJ indefinitely. In the case of suspects, the retention period for facial images depends on the seriousness of the offence and can be either 5, 10, 20 or 40 years. It also depends on whether the suspect is an adult or a minor. In addition, in the case of merged data entries for a particular person, the retention period associated with the most serious offence will apply. Photographs of unknown dead bodies are stored until the person's identity and the cause of death have been established, and the photograph of a missing person is retained until the person has been found.

Deletion of data (including facial images) takes place automatically according to the retention time set up in the system. However, there are situations (e.g. person is acquitted, accusation is dismissed etc.) when the data must be deleted before the retention period expires, upon a request from the justice services.

TAJ is also used for storing uncontrolled images (e.g. photo robot sketches, surveillance images etc.). The number of uncontrolled facial images was approximately 6000 out of 6 million images as of October 2019. Such images are attached to data entries for a specific crime and/or person, together with metadata about the offence (e.g. date and time, address, modus operandi etc.). These are retained in the database according to the legislation (the retention time depends on the seriousness of the offence or on whether the case has been solved).

1.4. Facial recognition searches

FR searches are performed by investigators of the National Police and the National Gendarmerie. Searches in TAJ are conducted with Cognitec Face VACS DBScan software. An upgrade from version 5.1.1. to version 5.4.1. was made in December 2019 and this has significantly raised the success rate of the searches.

Only frontal face images are suitable for FR searches. Controlled or uncontrolled images can be searched against the whole database.

No pre-processing is applied to probe images, but the quality of probe images is assessed by a FR algorithm, taking into account the following aspects:

- Partial occlusion of the face;
- Facial hair (beard, moustache, haircut);
- Glasses;
- Image overexposure or underexposure;
- Background noise;
- Image resolution (minimum interpupillary distance of 60 pixels);
- Degree of blur;

- Deviation of frontal position (±15°);
- Photo robot sketch.

An optimal response of the algorithm for FR searches is expected when a probe image contains a face with a distance of at least 150 pixels between the pupils. However, lower quality uncontrolled images can also be suitable for search purposes.

Search results are returned as a list with a maximum of 200 candidates (the actual number of returned candidates depending on the number of candidates above a set threshold), which may include more than one image for a given individual. The list is manually evaluated by the investigator conducting the search and no "lights out" approach is used. Currently, there are no specific criteria in use for a "match" decision and the investigator decides whether there is a likely candidate or not.

In 2018, approximately 200 000 searches were performed and a further 250 000 took place during the first eight months of 2019. No statistics are available regarding the number of "matches" and/or the "match rate".

FR is solely used as a tool to support investigations. The search results are not suitable as evidence in court.

1.5. Quality assurance

Instructions and quality requirements for the capture of controlled facial images are available in a written guideline for persons who carry out this task. Requirements are set for the following:

- Pose – head straight, ears visible (no hat, scarf, hair interfering with the photography), no glasses, eyes visible and open, mouth closed, neutral expression etc.;
- Distance – 1.5 to 2 m between the camera and the subject, 1 m between the wall and the subject;
- Background – clear and solid neutral background (white or grey at 18%) etc.;
- Lighting – no flash, white balance adjusted according to the shooting conditions etc.;
- Other – no use of digital zoom, 4/3 image format etc.

No quality requirements are set for uncontrolled images.

Several file formats are acceptable for both, controlled and uncontrolled images to be entered in TAJ. These are – JPEG (preferred format), PNG, BMP and GIF. Before enrolment into the FR system, photographs will undergo compression such that the maximum image size is 150 kB with a minimum resolution of 800 x 600 pixels. In addition, photographs are indexed by the FR software. This process includes the detection of the face on the image, localization of the eyes, image normalization (e.g. centring, positioning, size fixation) and extraction of the facial features. Written recommendations for image enrolment are also available and the personnel performing this work receive training.

No specific written methods have been developed for conducting FR searches. Some basic training is provided to the investigators of the National Police and the National Gendarmerie who are using the TAJ FR search functionality. However, at the present time, when it comes to the FR users, no systematic training is compulsory, no special skills are required and there is no proficiency monitoring.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The Criminal Procedure Code regulates the collection of facial images from the following groups of persons:

- Suspects – Article R.40-25 and Article R.40-26 1 °;
- Victims – Article R.40-26 3 °.

2. Civil databases

Facial images are taken and stored in several civil proceedings. Most commonly:

- For the issue of biometric passports, national identity cards and driving licences, which are the responsibility of ANTS (*Agence Nationale Des Titres Sécurisés*) [National Agency for Secured Documents];
- In relation to foreign nationals, which is the responsibility of DGEF (*La Direction générale des étrangers en France*) [General Directorate for Foreign Nationals in France].

Facial images that have been recorded for civil purposes cannot be used for FR within the current legal framework. Only in very exceptional circumstances, are the police permitted to ask for such an image for a manual 1:1 facial image comparison. From a legal point of view, the French data protection legislation makes it unlikely that civil face image databases (such as the identity document, driving licence, visa or aliens' databases) will be used for criminal investigation purposes.

Germany

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

Automated FR, in relation to criminal activity, has been in use in Germany since 2008. The facial image search facility is maintained by the *Bundeskriminalamt* (BKA) [Federal Criminal Police Office] as part of the criminal information system INPOL. The facial image database stored in INPOL contains 5.5 million mugshots. Individuals who are suspects, convicts, arrestees, missing persons, asylum seekers or wanted are stored in the INPOL system. While the facial image database is populated with images of individuals provided by police departments from across the country, the BKA is responsible for the maintenance of image quality in the system. In Germany, only qualified facial image examiners are permitted to conduct facial image searches. At this time there are 70 such examiners/experts in the country. Facial image search results are primarily used for police-related purposes. However, should the need arise, evidence can be presented in a court of law. Searching facial images that have been recorded for civil purposes, such as driving licences, passport applications, is neither technically possible, with current infrastructure, nor is it legally permitted for police forces. However, in exceptional circumstances, police forces are permitted to ask for access to an image in such a database, for a 1:1 examination to establish the identity of an individual. There are no permanently installed live search systems in Germany.

1.2. Organisations involved

Three levels of German policing are referred to in this report. These are: *Bundeskriminalamt* (BKA) [Federal Criminal Police Office], *Bundespolizei* (BPOL) [Federal Police] and *Landeskriminalamt* (LKA) [State Criminal Police Forces]. Among the main tasks of the BKA is maintaining the central police information system (INPOL). Each of the policing organisations mentioned contribute facial images and other data to INPOL. In return, BPOL and LKA have access to INPOL for, among other things, FR searches. Additionally, the BKA investigates threats to national security such as terrorism and/or other organised or large-scale crime that are beyond the resources of the regional departments.

The Federal Police is responsible for a variety of policing activities including border and coastline security, international airport security and the policing of the national rail network.

Each of the 16 independent states in Germany has their own State Criminal Police Office. The primary role of the state police departments is the prevention and investigation of criminal activity.

1.3. INPOL

Germany currently has one searchable national facial image database. The database in question is part of the criminal information management system known as INPOL (*INformationssystem POLizei*) [Information System of the Police]. With the application of Oracle software, the INPOL system holds information relevant to the police in accordance with legal regulations. The information held includes: name, aliases, date of birth, place of birth, nationality, fingerprints, mugshots, description of appearance, flag if DNA-information is available and information about prison sentences, if an individual is violent or armed and background information about criminal cases are also included.

The BKA has managed a facial image archive since 1972, however, at that time the archive was not electronically searchable. In 2008, a digital, searchable database of facial images was implemented. As part of the conversion process, all analogue facial images, held in the BKA archive, were scanned and stored in digital format. By the end of 2018, the German INPOL system held data on 6.2 million people, which included 5.5 million mugshots.

Each of the state police agencies maintains a local facial image database that is mirrored in the national INPOL system. Although these images are submitted to the national database, the regional departments retain ownership of the data provided. Regional databases can only be searched on a local basis. The central BKA and agencies from other states do not have access to the local databases of other states.

Currently, the German system requires that mugshot images are taken from the front, both sides, two 45-degree images and a full body image. There have been plans to increase the number of shots to be taken. However, these plans are currently on hold as the machine learning approach taken to FR has made the system more flexible in relation to pose deviations. There have also been experiments made with “video mugshots” (capturing moving images of an individual as part of the criminal registration process), however, it was decided that this process was too technical and expensive to be a practical option.

The registration of known individuals is conducted in a fairly standardised format, although there may be certain regional differences in the 16 federal states. The data collected includes: name, date of birth, place of residence, physical description, fingerprints and mugshots. Other than in certain very specific cases, DNA is not automatically recorded as part of the criminal registration process, although it can be taken at the discretion of the person being registered. Data collected during the registration process is checked against the INPOL database initially with fingerprints and only if necessary, with facial images.

Facial images of individuals suspected of having committed a criminal offence, arrestees, wanted persons, missing persons, individuals convicted of a criminal offence are enrolled into the INPOL system. These images are deleted from the system according to the legal framework when an individual is no longer of interest to the judicial system. In addition to crime related circumstances, images of asylum seekers are checked and stored in the INPOL system for a period of up to ten years. Images of asylum seekers are stored separately from the criminal database.

Uncontrolled images (e. g. images from CCTV cameras) may be stored in the database if these images are the only ones available.

1.4. Facial recognition searches

FR searches are performed by trained examiners at all three levels of German policing as described in Section 1.2. On the request of investigating officers, searches in the INPOL database are conducted with Cognitec Face VACS software. While most German states are solely using the INPOL database for FR searches, some use their own FR system to search regional databases in addition to the centralized one. Information in the following paragraphs about searches apply only to the INPOL database and not to the regional ones.

At this time, only frontal facial images are searched in the INPOL facial search system. However, there are plans to include side views and half-side views in the future. Facial image examiners only use the original or un-manipulated image for the comparison stage of the process.

Depending on the circumstances, the Cognitec system used by the German police will generally provide a candidate list of 10, 20 or 100 images. It is important to note that, due to multiple registrations a candidate list may involve the same candidate more than once. In certain circumstances, there are options available to increase the number of candidates listed to 1000.

Statistics show a match rate of 4.15% for the year 2019 (53 000 searches with 2200 matches). Due to the use case (candidate list that has to be verified manually) it is not possible to assess the match rate technically. The number of matches generated by facial comparisons is reported to the BKA annually.

At the BKA, facial image examiners provide a two-tier service. The first of these is a fast, firm indication of similarity between two images. Reports made at this level of examination are considered to be criminal intelligence, rather than a forensic examination. However, in certain circumstances this form of report can be used as evidence in court. The second tier of examination is a more involved form of forensic examination and comparison. This in general is a time-consuming in-depth process, and should an individual be identified with this process, a full forensic statement of identification will be written. Images are included in the report and matching features are marked on the images. The German judicial system does not allow for a categorical statement of identification to be made based on face comparison, rather statements to court are the combination of examiner opinion and a predetermined scale of conclusion ranging from a strong probability of exclusion at one end to a strong probability of inclusion at the other. Although the term probability is being used, no statistical calculations are made during this process. No report is produced without two concurring examiner opinions.

Regarding live searches, the Federal Police has only conducted research on this topic and a live test in a train station in 2018.

In addition, the *Bayerisches Landeskriminalamt* (BLKA) [Bavarian State Criminal Police] maintain a local facial image database that is used as a research and development tool as part of an ongoing project known as “Extended Use of Facial Recognition”. The purpose of the project is to test the flexible use and additional processing of images taken in the course of investigations conducted by the Bavarian police in a local FR system working independently of the federal database.

1.5. Quality assurance

There is little in the way of standardisation with respect to the type of cameras in use for taking mugshots. These range from a good quality digital single lens reflex camera to a camera that has been pre-installed into a registration suite. There are, however, technical and image quality requirements made of those conducting the registration. These include distance of the subject from the camera and lighting conditions. There are also image quality expectations. Images are stored in accordance with ISO standard 19794-5 (600/1200 x 800/1600 pixels) in JPEG format with a maximum compression factor of below 19. Telegray 4 (RAL 7047) with a tonal value of 18% is to be used as the background colour. A colour depth of 24 bits (in RGB mode) is used. Individuals wearing glasses, hats, caps, headscarves, wigs, toupees, etc. are photographed with and without these objects, and both sets of images are recorded.

Mugshots are primarily taken in a police station by trained police personnel. Images are taken according to SOPs. Alternatively, if an individual is convicted of a crime, mugshots can also be taken during a prison enrolment process. Although not a criminal registration, a single image is also taken of asylum seekers. Unaltered copies of all registration images and other relevant data are automatically uploaded as a single package to the INPOL database. Facial images are available for use within minutes of being uploaded to the INPOL system. Image quality is checked as part of the registration process during the enrolment. The officer that performs the enrolment is required to check that the image is suitable and in accordance with SOPs before sending images to the INPOL database. In order to mitigate the event of an image of poor quality being enrolled to the INPOL system, officers are provided with specific training both in the recording of fingerprints and facial images. The BKA is in the process of developing a fully automated quality control application for the facial image registration system.

Facial image searches are conducted by examiners and experts, who are in some cases recruited with the aid of an aptitude test in order to assess their abilities to both recognise faces and differences in facial features. Examiners have undergone an 11-week training programme and are trained in performing FR and facial image comparisons. Experts are examiners with an additional qualification in presenting the findings in court. Experts have to complete a two and a half to three-year training programme including courses and tests/exams provided by the BKA forensic establishment. The test/exam taken at the BKA includes 3 cases to be examined in three days (i.e. one case per day). Of these, one case will be presented by the trainee at a mock court session. At this time Germany has 70 qualified facial image examiners/experts.

In the Forensic Science Institute of the BKA, facial comparison and other forensic science examinations are conducted in accordance with DIN EN ISO/IEC 17020-2012 (Type A).

1.6. Legal framework regulating the use of facial images in relation to criminal activity

In German legislation, there is no differentiation made between facial image data and any other kind of biometric data. However, there are legal restrictions on what can be done with such data. These restrictions are regulated first, by national legislation and secondly, by regional laws at state level.

The most important legal acts at national level are:

- German Code of Criminal Procedure (*Strafprozeßordnung* – StPO) www.gesetze-im-internet.de/stpo/BJNR006290950.html
- Federal Police Law (*Gesetz über die Bundespolizei* – BPolG) www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html
- The Law on the Establishment of a Federal Criminal Police Office (*Bundeskriminalamtgesetz* – BKAG) www.gesetze-im-internet.de/bkag_2018/BJNR135410017.html

The above-mentioned law BKAG regulates the storage of data in BKA INPOL system.

On the state level, there are sixteen pieces of legislation in Germany, one for each state. For example, Hessian Law on Public Security and Order (*Hessisches Gesetz über die öffentliche Sicherheit und Ordnung* – HSOG):
www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?xid=169564,1

2. Civil databases

With some exceptions, civil databases in Germany are not managed by the national government. Instead, they are the responsibility of the local federal states. This means that there are 16 regional databases for each of the civilian databases that exist. These include:

- Passports/ID-cards (non-searchable archive of images). Until 2020, the only additional biometric data linked to passports and ID-cards in Germany were fingerprints that were included at the passport/ID-card holder's request. Since 2020, two fingerprints have been stored on the Passport/ID-card chip in accordance with EU requirements. Fingerprints taken for this purpose are not stored on any database or register.
- Driving licences (non-searchable archive of images). Driving licence images are only updated if a licence is renewed.

In certain circumstances it is possible to ask one of the civilian databases owners to provide an image in order to check the identity of a particular individual. These databases include:

- The database of foreigners (Federal database);
- Driving licence database (Local state database);

- Passport and ID-card database (Local state database);
- Short-term visa database (Federal database).

However, these systems do not have searchable databases and there are no FR systems running on them. Access to these databases is for 1:1 comparison only.

Greece

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

In relation to criminal investigations, automated FR has been used in Greece since 2019. For FR search purposes, a mugshot database is used. It contains facial images of about 377 000 individuals (i.e. suspects who have been arrested and convicts who have been sentenced to imprisonment). Facial images are captured in different police stations across the country and are sent for enrolment to the Video and Image Laboratory of the Audiovisual Evidence of the Department of Photography and Modus Operandi of the Hellenic Police Forensic Science Division, who is the custodian of the mugshot database. FR searches are performed only by facial examiners of the same unit. The number of examiners performing the searches is currently 4. The search results are primarily used for investigative purposes, but the results can also be used in court, if needed. Facial images that are collected and stored for civil purposes (i.e. in the course of various document applications) cannot be used for FR in criminal investigations. However, the police can request such an image for a manual 1:1 comparison.

1.2. Organisations involved

The Hellenic Police Forensic Science Division is responsible for the implementation and use of FR for the investigation of crime.

1.3. Mugshot database

The mugshot database is the only database in Greece that is used for FR searches for the detection, prevention, and investigation of crime.

The custodian of the mugshot database is the Video and Image Laboratory of the Audiovisual Evidence of the Department of Photography and Modus Operandi of the Hellenic Police Forensic Science Division. The software used for the database management and searching is Fire Exos II, produced by Unidas.

The mugshot database contains the facial images of suspects who have been arrested and of convicts sentenced to imprisonment. As of January 2020, the number of individuals with images stored in the mugshot database was about 377 000. An image can be stored in the database until the person reaches the age of 80 years but can be deleted sooner in a situation when the person dies or is acquitted. Multiple images of a person are captured and enrolled in the database:

- Frontal view image;
- Right side view image;
- Full body image.

Images are taken using special outfitted image capturing stations at the Hellenic Police Forensic Science Division, as well as using general custody rooms with a digital camera in police stations across the country (the number of such police stations in Greece is 70).

The enrolment of the images into the mugshot database is done by forensic examiners at the Hellenic Police Forensic Science Division.

Other biometric data (e.g. fingerprints) and biographic information (e.g. name of the person, nationality) are stored in separate databases. Mugshot images are linked to fingerprints and biographic data using a unique number.

Uncontrolled images are searched but are not stored in the mugshot database.

1.4. Facial recognition searches

At the present time, FR is carried out by forensic examiners of the Video and Image Laboratory of the Audiovisual Evidence of the Department of Photography and Modus Operandi of the Hellenic Police Forensic Science Division. The number of examiners is 4 (with 2 licences in use).

The Fire Exos II software from Unidas is used for both database management and for the searches.

Only frontal view images are used for FR. A probe image can be processed (with Photoshop) either before or after it has been enrolled by using filters, cropping etc. Both possibilities (processing before and after enrolling) are allowed and used in practice.

There are no strict rules set for the number of posts in the candidate list. The length of the list depends on the quality of the probe image as well as on each individual examiner. Thus, hundreds of candidates may need to be examined. There is no standardised threshold set for the search results and the criteria for a "match" is decided by the examiner. Also, the "lights out" scenario is not used.

The search results are reported as a "match", "likely candidate" or "no result". The most common reported result is "likely candidate". The results are reported to the prosecutors and the police for investigative purposes. However, the reported information can be used in court as evidence.

At the time of the interview, the FR system had been used for less than a year and therefore no annual statistics were available relating to the number of searches, the number of hits and the match rate.

Photographs from civil databases can be used for manual 1:1 facial image comparisons, but not for database searches.

1.5. Quality assurance

The quality requirements for image capture (e.g. lighting, background, pose etc.) have been described in written instructions for the personnel performing this task. Images are enrolled in JPEG format and must be at least 1–2 megapixels in size.

At the present time, there are no methods or SOPs in place for facial image enrolment and searches, but there are plans to develop these in the future. Individuals who enrol and search facial images have been trained by the company that has provided the face recognition system.

2. Civil databases

There are two major civil databases in Greece that contain facial images:

- Passport database;
- ID-card database.

These databases are not FR searchable for the investigation of crime. However, the police can ask for images for 1:1 facial image comparisons. Further, in situations when the identity of a document applicant is questionable, the forensic examiners can be requested to perform 1:1 comparisons.

2.1. Passport database

The Passport database is owned by the Hellenic National Passport and Secure Document Center. A passport, which can be issued from birth, is not a mandatory document in Greece.

The Passport database contains biographic data (date and place of birth, passport data, names, contact information) together with biometric data – facial images (frontal only) and fingerprints (from applicants of 12 years of age and above). The facial data is linked to fingerprints through a unique number.

About 3 million individuals are registered in the passport database, starting in 2006. Images are retained in the database indefinitely. If an image of a known individual is enrolled several times, all these images are stored in the database. No limits are set for the number of images per individual.

Images are taken only by professional photographers in accordance with specific instructions and the ICAO standard. A guideline can be found in English on the following website: www.passport.gov.gr. A recent photograph, printed on special paper is submitted by the person who applies for a passport. Only paper photographs are accepted at the present time. However, there is a plan that digital images will be accepted in 2022.

Enrolment is performed at the Hellenic National Passport and Secure Document Center. Passport offices across the country send applications to this division, where all application materials, including images are digitised by scanning. A step-by-step guide for this process has been developed, but no accreditation has been established. The accuracy of the application materials is verified by checking personal data against previous data, if it exists (e.g. the renewal of a passport). Approximately 2000 applications are enrolled daily. The individuals who enrol the facial images into the database receive on-the-job training.

There is no link between this database and any other external databases.

2.2. ID-card database

The owner of the ID-card database is the State Security Division / Identity Cards & Archives Section of the Hellenic Police Headquarters. The ID-card database contains facial images from 8 to 9 million individuals and 15 million photographs (frontal only). Images are retained in the database indefinitely. If an image of a known individual is enrolled several times, all these images are stored in the database. No limits are set for the number of images stored per individual.

The capture of images is done by professional photographers according to specific guidelines published on the Hellenic Police website. The image requirements include dimensions, background colour, distance and pose. The photographs are submitted by applicants printed on special paper and these are digitised by scanning at police stations across the country (approximately 360 stations). No SOPs or training is in place for this procedure. A verification of the accuracy for the application data is performed by checking personal data against previous data, if that exists. This includes a cross-check with data in the Civil Registry databases of municipalities.

Alongside images, a name, surname, names of parents, date and place of birth, ID-card number, issuing authority etc. are stored in the database. No other biometrics (i.e. fingerprints) are collected for the issue of ID-cards.

Hungary

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

FR has been implemented in Hungary since March 2016. The use of FR is regulated by the Act CLXXXVIII of 2015, Facial Image Analysis Register and Facial Image Analysis System that stipulates the use cases of FR, a database used for FR searches (i.e. Facial Image Registry) and data sources for this database.

Currently, the data sources for the Facial Image Registry are databases that contain facial images of individuals of known identity from various document/civil proceedings. In the future, the Registry of criminal records database that contains facial images (i.e. mugshots) for those holding a criminal record, is also planned as a data source for FR.

While several institutions capture and enrol images, only one organisation, i.e. Hungarian Institute for Forensic Sciences is authorised to perform FR searches.

Uncontrolled images related to criminal activity (e.g. CCTV camera footage) and individuals of unknown identity are not stored in any database. However, such images can be submitted for image analysis and searches against the Facial Image Registry.

1.2. Organisations involved

The Hungarian Ministry of Interior is responsible for the Facial Image Registry and for the use of FR in criminal investigations. The data sources from which images are transferred to the Facial Image Registry (and thus, are used for FR searches) are owned by the Ministry of Interior. Image analysis and searches are performed by the Hungarian Institute for Forensic Sciences.

1.3. Databases of facial images that contain facial images and are used for facial recognition in relation to criminal activity

According to the Act CLXXXVIII of 2015 Facial Image Analysis Register and Facial Image Analysis System Article 1, the registers in Hungary that are permitted to be used as data sources for FR for the prevention and detection of crime, for the apprehension and prosecution of perpetrators, for the identification of convicts and persons held in custody, as well as for the identification of dead bodies and searches for missing persons are as follows:

- Data register of identity documents;
- Data register of passports;
- Data register of road traffic;
- Asylum Information Database;
- Central Aliens Policing Registry's sub-registries:
    - Central National Visa System;
    - Residence permit and permanent residence permit registry (including temporary residence certificates);
    - European Economic Area documents registry.

The first three registers listed above are administered by the Deputy State Secretariat for Data Registers and the last two registers are administered by the National Directorate-General for Aliens Policing.

All the above-named source databases contain biographic data (name, surname, etc.) alongside the facial images. Other biometric data (fingerprints) are taken and used only for issuing documents and are not stored in any database. The biographic data of a document application is checked and confirmed by presenting a previous document, thus eliminating duplication due to aliases.

Images collected and stored in the above-named databases are from applicants for ID-cards (a mandatory document for Hungarian citizens from 16 years of age), passports, driver's licences, visas, residence permits (temporary/permanent), and also from those applying for international protection.

Photographs for ID-cards, passports and driver's licences are taken using specially equipped image capturing stations at document offices across the country. Photographs for documents issued by the National Directorate-General for Aliens Policing are taken either at consulates, regional directorates of the National Directorate-General for Aliens Policing or the asylum authority. Equipment used to capture images varies from cameras to photo booths.

The type of image that is captured is a frontal view image and the file format used is JPEG. All photographs are taken in accordance with ICAO standards. In addition, a written document called "A Methodical Guide on the Technical Equipment to Use in the Document Office and the Requirements for Portrait Photography" is in use for the capturing and enrolment of images.

Images in the above-named databases are stored for 5 to 25 years depending on the purpose for which the image was taken.

There may be multiple images of a person in different databases that are used as data sources for the Facial Image Registry. Thus, the Facial Image Registry may contain more than one image per person.

1.3.1. Facial Image Registry

The Facial Image Registry is an image gallery for performing FR searches. It is synchronised with the source databases listed in Section 1.3. The Facial Image Registry contains facial images, biometric templates of facial images and a reference to a source database. Currently, it contains approximately 30 million templates. No other data (e.g. biographic information) that is stored in the source databases is available in the Facial Image Registry.

1.4. Facial recognition searches

The search engine used for FR was purchased from and implemented by NEC. The searches are performed by analysts of the Hungarian Institute for Forensic Sciences (HIFS). The number of analysts is 27 who, in addition to facial image searches, carry out manual 1:1 facial image comparisons.

According to the Act CLXXXVIII of 2015 Facial Image Analysis Register and Facial Image Analysis System Article 9, the following authorities can submit search requests:

- National Investigation Agency;
- Criminal Courts and the Prosecution Service;
- National Protective Service;
- Counter-Terrorism Centre;
- Hungarian Prison Service;
- The body conducting the criminal proceedings;
- The Public Administration;
- Special Service for National Security;

- Intelligence Agencies;
- Police;
- The Parliamentary Guard;
- The Hungarian authority who provides Legal Aid;
- Witness Protection Service;
- National Directorate-General for Aliens Policing;
- The authority dealing with citizenship matters.

As of February 2020, 8615 people are allowed to submit search requests, 7924 people can view search results and 1121 people are mandated to submit urgent requests.

The requesting authority submits a questioned image to HIFS to be searched against the Facial Image Registry. Usually, these images are still images from CCTV footage. Analysts at HIFS make biometric templates from the images received and perform the database searches.

As a rule, a list with 1000 candidates is returned and processed. Nevertheless, the number of posts in the candidate list can be changed by the analyst depending on the specific case. Further, the candidate list can include several images of the same person. The candidates are evaluated by human. No specified score threshold for the match value and no "lights out" computer-based evaluation is used. The decision, whether there is a match or not, is made by more than two FR analysts. Two analysts, independently from each other, perform the search, come up with a candidate list and evaluate the candidates. Both lists are sent to a lead analyst, who makes the final decision.

Results are reported back to the requesting authority either as a "match" or "no match" within 8 working days from receiving a search request. In the case of a "match", the candidate(s) is/are sent to the requester as a reference described in Section 1.3.1. Biographic data of a person of interest can then be accessed in the source database using the reference number. In the case of "no match", information that the search ended in no potential candidates is presented.

FR search results are used only as an investigative lead and they cannot be used as evidence in court.

1.5. Quality assurance

The following measures have been applied to ensure the quality of FR work:

- First level – law that stipulates the use of FR (Act CLXXXVIII of 2015 Facial Image Analysis Register and Facial Image Analysis System) and detailed rules for the operation of the facial image analysis system (Decree 78/2015 (XII. 23.) of the Ministry of Interior).
- Second level – applying of ICAO and ISO / IEC 19794-5 standard by using written instructions called "A Methodical Guide on the Technical Equipment to Use in the Document Office and the Requirements for Portrait Photography".
- Third level – training of personnel working with equipment that is used for image capturing, and software that is used for databasing and FR searches.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The most important legislative acts that regulate the use of FR in relation to criminal investigations are:

- Act CLXXXVIII of 2015 Facial Image Analysis Register and Facial Image Analysis System that stipulates the content of Facial Image Registry, access rights, analysis process etc.

https://net.jogtar.hu/jogszabaly?docid=A1500188.TV

- Ministry of Interior Decree 78/2015 (XII. 23.) that stipulates detailed rules for the operation of the facial image analysis system https://net.jogtar.hu/jogszabaly?docid=A1500078.BM

Data collection of facial images from the source databases are regulated by respective sectoral laws.

2. Database of facial images that is planned to be used for facial recognition in relation to criminal activity

An additional source database that is planned to be used for FR is the Registry of criminal records owned by the Ministry of Interior.

The Registry of criminal records contains personal data and criminal case data. The personal data includes biographic data:

- Surname and forename, previous surname and forename;
- Surname and forename at birth and, if there is a change, previous surname and forename name at birth;
- Gender;
- Place and date of birth;
- The mother's birth name and surname and, in the event of a change, her mother's previous birth name and surname;
- Personal identification number;
- Nationality, previous nationality;
- Address and, in the event of a change, previous address

alongside the photographs (although, not all criminal records include photographs). Information about the collection of other biometric data (fingerprints and DNA) is also available in this registry, but the respective data is stored in dedicated databases.

Images in the Registry of criminal records are from:

- Convicted offenders;
- Suspects;
- Persons who are subject to travel restrictions abroad.

The following images are taken:

- Front view facial image;
- Right side view facial image;
- Left half-side view facial image;
- Two full body images – one from the front and one from the left side.

Photographs are taken by forensic technicians employed by the investigating authority, designated and trained members of the investigating authority or by designated and trained members of the Prison Service.

If photographs of a known individual have been taken several times, all images are kept in the database. Photographs are stored as long as the criminal record is required to be kept according to the law. Afterwards, photographs will be permanently deleted. As of February 2020, the number of known individuals in the database was about 540 000.

3. Recent developments

Since the data collection interviews in February 2020 (as of September 2020), the following developments have taken place:

- A Nova.Mobil application has successfully been launched for police officers, which helps to identify someone who does not have any identification documents with him/her, by taking a picture of the person and searching that picture against the Facial Image Registry (i.e. 1:N search). As a result, a list of five candidates with reference numbers is returned. Based on the reference number, biographic data of the person of interest can be obtained.
- An automatic verification of applicants has been included in the renewal process for identification documents (i.e. ID-card, passport or driver's licence). During this process, an image of an applicant is compared 1:1 against his/her previous document photo in the Facial Image Registry.

Ireland

1. Facial recognition in relation to criminal activity

FR has not been implemented in Ireland at the present time. The principal reason for this is the legal restrictions that exist within the country, including the fact that it is not legally permitted for facial images collected for other purposes (e.g. passports, driving licences) to be shared in criminal investigations. There are also press reports over 2019–2020 that point towards general reservations from the Irish public about the capture of facial images in public places. Thus, there are no current plans within Ireland to move ahead with the use of FR for law enforcement purposes.

2. Civil databases

The information provided indicates that there are three areas where the Irish state stores facial images in electronic databases:

- Passports (Department of Foreign Affairs);
- Public Services Cards (Department of Social Protection);
- Driving Licences (Department of Transport).

Italy

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

FR in relation to criminal investigations has been implemented in Italy since May 2017, where images of unknown perpetrators are searched against the AFIS database of facial images. The AFIS is the only database that can be searched with a FR system. It contains facial images from various groups of people and the number of searchable images in the AFIS is about 10 million.

FR searches are currently performed by two police organisations, the National Police and the Carabinieri. Any police officer from these organisations can use the FR system to make a search for investigative purposes, but to use the results in a court requires a report from the forensic services.

There are no current plans to include any other databases for FR searches.

In addition, the police can ask for the image of a person of interest from another database (including civil databases) for manual 1:1 facial image comparison, but it is not allowed to perform FR searches in civil databases for the purpose of criminal investigations.

1.2. Organisations involved

Forensic Institute, National Police (*Servizio Polizia Scientifica, Polizia di Stato*):

- Custodian of AFIS;
- Performer of FR 1:N searches;
- Performer of forensic 1:1 facial image comparisons;
- Capturer of mugshots.

Carabinieri (*Arma Dei Carabinieri*):

- Performer of FR 1:N searches;
- Performer of forensic 1:1 facial image comparisons;
- Capturer of mugshots.

Financial Guard (*Guardia di Finanza*):

- Capturer of mugshots.

1.3. AFIS facial image database

In Italy, the database of facial images that is used for FR searches is AFIS. The National Police is the custodian of the AFIS facial image database (more specifically, the Forensic Institute). The AFIS software is from Thales (previously Cogent). The persons that are entered into the AFIS facial image database are those who can be entered according to the law, e.g. convicts, arrested suspects, unidentified persons, immigrants and asylum seekers. About 90% of the AFIS subjects are foreigners, that are thereby available for FR searches in criminal investigations.

The AFIS facial image database contains about 9 million individuals and 17 million images. There is no limit to the number of times the same person can be enrolled.

In addition to facial images, also fingerprints are stored in AFIS, while DNA is in a separate database. The facial images in AFIS are linked via fingerprint to the same identity. The facial data contains both a frontal image and a right profile image of each person.

There are three police organisations in Italy who take mugshots: the Carabinieri, the National Police and the Financial Guard. The mugshots are taken, together with fingerprints, at the police stations distributed across the provinces and even at smaller facilities within the organisations (the Carabinieri has around 400 booking stations for mugshots). The mugshots are taken with specialised stations for image acquisition called *Identy System*. A room with uniform lighting and background is used, and two digital cameras (a frontal and a right profile) take images simultaneously. In addition, the person's height is measured. The personnel are trained to capture images and use the special equipment to achieve images of uniform quality. There are no written instructions, but the different steps are built into the *Identy System* and must be followed.

The fingerprints and facial images are then enrolled into AFIS, where fingerprints are used to check whether the person is already in the AFIS system or not. Any new entry gets a unique identity code, but if the person is already in AFIS the new mugshot will be linked with the existing code. The enrolment is mainly done by forensic experts. The training for enrolment is part of a more general training for fingerprints, photographs, fingerprint comparison, facial comparison etc.

At the present time, the images are saved in JPEG format, using lossy compression. These new photographs are of a homogenous quality as they use the same *Identy System* for capture. There was no standard used for photographs captured in the past.

Together with the biometric data in AFIS, metadata is stored, e.g. name, place of birth, date of birth, name of father/mother, description of facial features (eye, hair colour etc.), scars, marks, tattoos (images are included for tattoos) and the reason why the person was entered into the database.

Uncontrolled images are not stored in the AFIS facial image database.

1.4. Facial recognition searches

FR searches against the AFIS facial image database by the National Police became operational in May 2017, and then by the Carabinieri in 2018. There are two search engines implemented, one from NEC (NeoFace Watch software) and the other from Reco. The system is designed to be independent of the specific engine being used and it is possible for the user to select which of the two engines to use.

At the present time only 10 out of the 17 million AFIS images can be used in the FR system due to a licence limitation. Consequently, the FR system is limited to include only mugshots from the last 15 years and a maximum of three images per subject (the last three). Also, only the frontal images can be searched.

The National Police has approximately 6000 licences, while the Carabinieri has 150. The searches are mainly done by police officers for investigative purposes, but also by forensic experts in situations when police officers do not have the access to perform the searches themselves.

There are no specific restrictions on probe image quality, but the software sometimes does not accept the probe image because of poor quality. Sometimes pre-processing of the probe image is done, mainly cropping because the crop function is built into the FR system. Forensic experts usually have access to Photoshop, and sometimes attempt additional filtering to achieve better search results. The number of posts in a search result is 50 candidates, and there is no score threshold used. If the same person exists as several entries in the database, the software can group all these as one single candidate in the search result, which is ranked according to its highest score value. The user cannot change the search parameters, only an administrator. No “lights out” scenario is used.

The term “match” is not used, instead there is a manual confirmation of the search results to decide whether there is a potential candidate or not. The investigator can use the results for investigative purposes, but if there is a need for a further confirmation or to use the result as evidence to court, a 1:1 facial image comparison by a forensic expert is requested. If the original search is done by a forensic expert, on the other hand, a likely candidate is reported when such a result is found. In general, the FR search results cannot be used in court, only 1:1 facial image comparison reports provided by the forensic services.

At the National Police, the forensic 1:1 facial image comparison is performed according to the ENFSI DIWG best practice manual, and is reported according to a verbal conclusion scale ranging from grade -3 to +3. There is no likelihood ratio (LR) calculation involved in this evaluation.

At the Carabinieri, in some cases the FR search results from the investigator are sent to the forensic experts to decide if any of the candidates on the list is of interest. A forensic 1:1 facial image comparison is then made, and is reported back to the person who requested it, or to the prosecutor. The Carabinieri uses a verbal scale consisting of: limited support, moderate support, light support, strong support and very strong support. Since 2020, they have also implemented a score-based-likelihood ratio approach in collaboration with the University of Catania from which a LR is computed from the FR score. The LR is given together with the verbal conclusion in the forensic report, but experience has shown that judges do not understand the concept of LR and for this reason, the verbal scale is preferred. The Carabinieri does around 400 1:1 comparisons per year.

1.5. Quality assurance

No quality standard is currently used for the facial images in AFIS and there are no plans at the present time to implement a quality standard. However, it is planned to implement an automatic quality check at the capture stage, but this is still at a testing phase. Even when implemented, the operator will be able to override a bad quality warning when necessary for operational reasons. There is an ongoing discussion about improving the quality of the mugshot images, mainly to reduce compression and enhance image resolution. Also, to improve data quality in the future, collaboration with academics is underway to implement a multi-camera system to include 3D facial information in the database.

There are no specific requirements for recruitment of the personnel who run FR searches. There is basic training available for operators on how to use the FR software, including some insights into how the results can be used and when to ask for a forensic 1:1 facial image comparison. Only the 1:1 facial image comparison forensic experts participate in proficiency testing.

2. Civil databases

Facial images for civilian use in Italy are collected from document applicants of national ID cards, passports and driving licences. Issue of ID cards and passports is under the responsibility of the Ministry of Interior, while driving licences are issued by the Vehicle Registration Office governed by the Ministry of Transportation.

The police can ask for the image of a person of interest from a civil database, but it is not allowed to perform FR searches in civil databases for the purpose of criminal investigations.

Latvia

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

The implementation of FR in Latvia begun in 2009, when the Biometric Data Processing System (BDAS) Law was adopted and then, FR became fully operational in 2012. BDAS is used as a central biometric repository to store facial and fingerprint data collected by state institutions during different civil and criminal proceedings. Biometric data related to crime investigation is stored in a logically separated sub-database of BDAS referred to as the criminal data array. The BDAS criminal data array contains information obtained from detained, suspected, accused and convicted people and also from unidentified dead bodies. As of January 2020, there were more than 270 000 cases registered in the BDAS criminal data array and approximately 78 000 of these included facial images.

Only information in the criminal data array is used for FR searches during crime investigations, while all other sub-databases are unavailable because of both technical and legal restrictions. It is permissible for FR searches to be conducted by a wide range of police officers, when needed, during criminal investigations. The results of the search can only be used as an intelligence lead.

1.2. Organisations involved

The Information Centre of the Ministry of Interior is the owner and custodian of BDAS. The State Police of the Ministry of Interior is the user of information in BDAS both in terms of entering the data and performing FR searches.

1.3. Criminal data array of the Biometric Data Processing System

Biometric Data Processing System involves the following sub-systems:

- Criminal data array;
- Civil data array;
- Asylum and migration data array (so called Eurodac array);
- AFIS.

All the data arrays are logically separated from each other. The software for the database management is from the RIX Technologies.

Only the criminal data array is described in more detail in this section as it is the only sub-database in BDAS used for FR during criminal investigations. The civil data and Eurodac arrays of BDAS will be addressed in Section 3.

The BDAS criminal data array is comprised of information acquired during investigative activities from detained, suspected, accused and convicted people and from unidentified dead bodies. As of January 2020, there were more than 270 000 cases registered in the BDAS criminal data array and approximately 78 000 of these contained facial images.

Alongside the digital photographs of the face and fingerprints, the following non-biometric information is stored in the criminal array of BDAS for controlled images:

- Full name;
- Date of birth;
- Personal identity number (if such has been attributed);
- Nationality and its type (citizen, non-citizen, resident);

- Gender;
- Legal qualification of a criminal offence;
- Criminal case number;
- Justification for obtaining biometric data;
- Institution that acquired the biometric data;
- Date the biometric data was obtained.

Biometric and non-biometric data is always collected in parallel during a process which starts with the recording of biographic information. After this, photographs are taken, using a single-lens reflex camera with a resolution of at least five megapixels. The photography is followed by the collection of the fingerprints.

An automatic check of the biographic and biometric data is always performed before the data is entered into BDAS. All cases with mismatches between previous and current data are followed up.

If a person's data (all data or an individual data entity) is collected on more than one occasion, the data that was initially stored is replaced when the new data complies with the BDAS quality requirements and is of better quality than the previous data.

During enrolment of facial images into BDAS, a built-in quality assessment tool checks the quality of images and their compliance with the minimum requirements set in the system. Facial images must correspond to the requirements of ANSI/NIST ITL-1:2011 and ISO/IEC 19794-5 Part 5: Face image data. Images of insufficient quality are rejected by the system. For instance, quite often digital images of an unidentified dead body do not meet the quality requirements and the facial data is absent from the database.

The criminal data array of BDAS can be used by the police for the following purposes:

- Detection of criminal offences and search for persons who have committed a criminal offence;
- Prevention of criminal offences and other infringements of the law;
- Verification of the identity of detained, suspected, accused and convicted persons;
- Determination of the identity of a person during intelligence activities;
- Biometric identification of unidentified dead bodies;
- Searching for missing persons.

Data obtained as a result of the investigational activities are stored in BDAS for 75 years. Data relating to unidentified bodies is stored for 5 years.

Uncontrolled facial images are not stored in the criminal array of BDAS.

1.4. Facial recognition searches

MorphoTrust ABIS Search Engine (version 6.5.1) is used for FR searches. Currently, only very good-quality images can be searched against the database. Images obtained from video surveillance cameras cannot be used for searches in most cases, because of insufficient quality.

A wide range of persons working for law enforcement have the right to use the criminal array of BDAS, and are allowed to perform FR searches and evaluate the candidate lists. The search results can only be used for intelligence and operative purposes and cannot be used in courts *per se*. If 1:1 facial image comparisons are needed, these are performed by forensic experts.

Statistical data on the number of searches performed and matches obtained is not available.

1.5. Quality assurance

The quality of facial images is checked automatically during the enrolment by the software component L1 (MorphoTrust Foundation SDK 8.7). Parameters evaluated are as follows: texture, exposition, face recognisability, contrast, centring and resolution.

Written instructions are provided to the personnel that capture facial images.

Training for FR searches is provided, on demand, for persons performing this activity.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

List of the most relevant legislative acts:

- Biometric Data Processing System Law
https://likumi.lv/ta/id/193111-biometrijas-datu-apstrades-sistemas-likums
- Personal Data Processing Law
https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law
- Criminal Procedure Law
https://likumi.lv/ta/id/107820-kriminalprocesa-likums
- The Sentence Execution Code of Latvia
https://likumi.lv/ta/en/en/id/90218-the-sentence-execution-code-of-latvia
- Regulations Regarding Biometric Data Processing System
https://likumi.lv/ta/en/en/id/266013-regulations-regarding-biometric-data-processing-system

2. Other databases and registers related to criminal activity that are not used for facial recognition

Besides BDAS, facial images are also stored in the Integrated Information System of the Interior, supervised by the Information Centre of the Ministry of Interior. The integrated system contains the following sub-systems that are used for storing information related to criminal activity:

- Single Register of Events;
- Register of Criminalistic Characterisation and Photographs of Persons.

The images in these databases are not searchable using FR tools.

2.1. Single Register of Events

The Single Register of Events is used by the state police, municipal police and port police.

The data entered in the register includes:

- Information on the event;
- Information on the person submitting information;
- Information on persons who have been, or may have been, caused financial, physical or moral harm;
- Information on persons who may provide information regarding the circumstances and nature of the event;
- Information on damaged, illegally alienated, removed, lost or found property related to the event;
- Photograph of the person who is examined in relation to causing (committing) the event.

Data in the Single Register of Events is stored for 10 years.

2.2. Register of Criminalistics Characterization and Photographs of Persons

The Register of Criminalistics Characterization and Photographs of Persons hosted and supervised by the Information Centre of the Ministry of Interior was established in 2012. It contains data on detained persons, arrested persons and persons who have been convicted with deprivation of liberty. Altogether, the register contains information on more than 49 000 registrations. Data is entered into the database by the prison administration and by the police.

Alongside other information, the following images of people are entered into the database: frontal view facial image, right profile and left 45-degree half-profile of the face, full body photograph with a ruler visible in the background, as well as photographs of tattoos and other special features.

The types of images stored and technical requirements, as well as the scope of information, requirements for inclusion and deletion of information, storage time and institutions allowed to access the register are determined by the Regulations of the Cabinet of Ministers, 02.10.2012 No 673 "Regulations Regarding the Register of Criminalistic Characterisation and Photographs of Persons" (https://likumi.lv/ta/en/en/id/251860-regulations-regarding-the-register-of-criminalistic-characterisation-and-photographs-of-persons).

3. Civil databases

Civil databases in Latvia are divided into two categories:

1) Databases used for issuing civil documents:
   - Information System for Personal Identification Documents (PADIS);
   - State Register of Vehicles and Their Drivers.
2) Databases related to border control:
   - Electronic Information System of the State Border Guard (REIS);
   - Information System of Fingerprints of Asylum Seekers.

Both, PADIS and the State Register of Vehicles and their Drivers are linked to BDAS and images obtained during the issue of documents are transferred to the civil array of BDAS. As of January 2020, there were approximately 2 million cases registered in the civil data array and 98% of them contained facial images.

The following information is included for a person in the civil data array:

- Frontal image of the face;
- Fingerprints (two fingers) of persons who apply for an identity document;
- Given name (names) and surname;
- Personal identity number;
- Gender;
- Nationality and its type;
- Fact of death of a person.

Face images that are added to the civil data array of BDAS must correspond to BDAS requirements regarding frontal face images.

3.1. Information System for Personal Identification Documents

The Information System for Personal Identification Documents (PADIS) contains information collected during the issue of identity cards and passports. Latvian citizens and non-citizens from 15 years of age must have at their disposal at least one valid personal identification document – a passport or an identity card. Starting from 1 January 2023, the identity card will become a mandatory personal identification document for Latvian citizens or non-citizens who have reached the age of 15.

Several types of passports and identity cards are issued:

- Identity card of a citizen of Latvia;
- Identity card of a non-citizen of Latvia;
- Identity card of a citizen of another EU Member State, State of the European Economic Area or the Swiss Confederation;
- Identity card (residence permit) of a third country citizen;
- Identity card of an employee of a foreign diplomatic or consular representation accredited in Latvia, international organisation or its representation, another subject of international law, consular institution or a family member or private housekeeper of such employee;
- Passport of a citizen of Latvia;
- Passport of a non-citizen of Latvia;
- Diplomatic passport;
- Service passport;
- Travel document of a stateless person;
- Travel document of a refugee;
- Travel document of a person to whom alternative status has been granted in the Republic of Latvia.

PADIS is hosted by the Office of Citizenship and Migration Affairs of the Ministry of Interior. Information in PADIS is added by the officials working for the Office of Citizenship and Migration Affairs or the Ministry of Foreign Affairs. Currently, PADIS contains information on 2.5 million persons. Facial images of Latvian citizens are stored from 2002, non-citizens from 1997.

Photographs are taken, registered and submitted at client service halls by the employees of the Office of Citizenship and Migration Affairs in Latvia and at the consular or diplomatic missions by the employees of the Ministry of Foreign Affairs in foreign countries. The facial images are obtained using an equipment and software solution produced by Vision-Box.

Frontal face images are entered into the database together with a person's name or names, surname, personal identification number, nationality, gender, date of birth, place of birth, height (cm), ethnicity, information on previous personal identification documents, institution issuing the document, information on person's children younger than 18 years, fingerprints and signature.

Employees receive individual training when starting to work with PADIS.

The most important legal documents regulating the field:

- Personal Identification Documents Law https://likumi.lv/ta/en/en/id/243484-personal-identification-documents-law
- Regulations Regarding the Information System for Personal Identification Documents https://likumi.lv/ta/id/294004-personu-apliecinosu-dokumentu-informacijas-sistemas-noteikumi
- Regulations Regarding Personal Identification Documents https://likumi.lv/ta/en/en/id/244720-regulations-regarding-personal-identification-documents

3.2. State Register of Vehicles and Their Drivers

As of August 2019, the State Register of Vehicles and Their Drivers contains information on approximately 900 000 persons that have received driver's licences, driving learner's permits, bicycle driver's licences, hazardous waste transport driver's licences or driver's qualification cards. The register is hosted and supervised by the Road Traffic Safety Directorate under the Ministry of Transport.

The following information is stored for each person while issuing the document:

- Frontal view facial image;
- Name;
- Personal identification number or date of birth;
- Address;
- Nationality and its type;
- Information on the personal identification document;
- Signature.

Photographs are taken, registered and submitted by employees of the Road Traffic Safety Directorate. Images are taken and processed using photo cameras CANON 1100 and FDSK Face Recognition Software.

Data entered into the register is stored permanently.

The most important legal document regulating the field is the Regulations of the National Register of Vehicles and Their Drivers (https://likumi.lv/ta/id/306566-transportlidzeklu-un-to-vaditaju-valsts-registra-noteikumi).

3.3. Electronic Information System of the State Border Guard

Electronic Information System of the State Border Guard (REIS), hosted and managed by the State Border Guard, contains information on persons crossing the external borders of Latvia and their travel documents, as well information on vehicles driven by persons crossing the border and their documents. As of February 2020, REIS contains information on 84 million border crossing events, 19 million traveling documents and 30 million facial images.

Based on the results of a risk analysis for a person crossing the external border, the biometric data (facial image or fingerprints) may be stored in REIS. The facial data is obtained by officials of the State Border Guard during a check of the person's document. The facial image is read from the microchip of the travel document with a special document examination device. The frontal view image must be in accordance to requirements of ICAO 9303 (www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Portrait%20Quality%20v1.0.pdf).

The information is usually stored in REIS for 5 years, after which it is automatically deleted. REIS is not linked with other biometric databases. FR searches are not performed. Also, it is not permissible to use REIS for FR searches in criminal proceedings. However, this may change in the coming years due to the implementation of a common Entry Exit System (EES), which provides the possibility for law enforcement authorities in criminal investigations to conduct searches against facial images and fingerprints registered in the EES.

The most important legal document regulating the field is the Regulations Regarding the Electronic Information System of the State Border Guard (https://likumi.lv/ta/en/en/id/298872-regulations-regarding-the-electronic-information-system-of-the-state-border-guard).

3.4. Information System of Fingerprints of Asylum Seekers

The Information System of Fingerprints of Asylum Seekers is part of BDAS and is also known as BDAS asylum and migration data array or a so-called BDAS Eurodac array. The information system contains data on persons seeking refugee or alternative status, detained third country nationals or stateless persons who are at least 14 years old. As on January 2020, the system (BDAS Eurodac array) contains around 2000 cases.

The information system is mostly used by the State Border Guard, but access is also granted to the State Police and to the Security Police.

Data is entered into the information system within 48 hours after an application for refugee or alternative status is received or after a person is detained. The data is thereafter sent for inspection/registration in the Eurodac Central System. Currently, only fingerprints are being processed by Eurodac, but given that future changes are planned, it is expected that FR searches (1:N) will soon be possible.

Data added to the Latvian system includes, among other information, a set of facial images – frontal view, right profile and left profile. If a person wears glasses for vision correction – frontal view, right profile and left profile with glasses is also included.

In accordance with the Eurodac Regulation, CAT1[24] records are stored for ten years and CAT2[25] records for 18 months.

[24] CAT1- Eurodac data acquisition category - International protection applicants

[25] CAT2 - Eurodac data acquisition category - Third country nationals or stateless persons detained in connection with illegal crossing of an external border

Lithuania

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

FR in relation to criminal investigations has been in use in Lithuania since 07.11.2019. Preparations for FR implementation started in 2013, when the Order of the Minister of Interior No 1V-440 “Regulations of the Habitoscopic Data Register” was adopted and the Habitoscopic data register was established. The implementation took place between November 2018 and November 2019 in a project called “Modernizing Habitoscopic Data Register using Advanced Personal Face Recognition and Personal Search Engine Identification Technology” conducted by the Information Technology and Communications Department under the Ministry of Interior. The next step in FR work will be the implementation of standards ISO/IEC 19794-5 and ISO/IEC FDIS 39794-5.

A FR search capability has been introduced in the Habitoscopic Data Register (HDR), which is the only system used for FR. The HDR stores images of suspects, convicts and arrested persons registered in HDR, and images of wanted persons, unidentified dead bodies and unidentified helpless persons registered in a database known as the Register of wanted persons, unidentified corpses and unidentified helpless persons (RPSUCUHP). As of December 2020, the HDR contains more than 400 000 facial images and the number of individuals registered in HDR is approximately 185 000.

FR is used for crime prevention and forensic examination as well as in the identification of wanted, missing and unidentified persons. FR searches can be performed by more than 500 police officers and forensic experts, to whom access to HDR FR module has been granted. As the implementation is very recent, FR searches are not yet performed routinely and hence, the current user experience is limited. Moreover, live facial recognition searches are not performed in Lithuania at the present time.

Regarding facial images of civil origin (i.e. from various document proceedings), it is permissible for law enforcement to use such images for manual 1:1 comparisons or 1:N searches against HDR. An automated search capability with the current infrastructure is neither permitted nor technically possible within civil databases.

1.2. Organisations involved

- The Information Technology and Communications Department under the Ministry of the Interior of the Republic of Lithuania ensures the proper functioning of the HDR and is responsible for the security of the data and coordinating or performing the maintenance work and improvements to the HDR technical tools and software.
- The Lithuanian Criminal Police Bureau enrols persons subject to preventive measures, persons in temporary custody suspected of having committed a criminal offense, wanted persons, images of unidentified persons recorded at crime scenes and in the investigation documents.
- The Police Department enrols persons subject to preventive measures, persons who have been served with a notice of suspicion of having committed a criminal offense and persons in temporary custody suspected of having committed a criminal offense.
- Territorial police institutions enrol persons subject to preventive measures, persons in temporary custody suspected of having committed a criminal offense, wanted persons and images of unidentified persons recorded at crime scenes and in the investigation documents.

- The Lithuanian Police Forensic Science Centre performs registration of images of unidentified persons recorded at crime scenes and in the investigation documents.
- The State Border Guard Service enrols persons who have been served with a notice of suspicion of having committed a criminal offense, persons in temporary custody suspected of having committed a criminal offense, wanted persons, aliens who have been apprehended by the competent control authorities and images of unidentified persons recorded at crime scenes and in the investigation documents.
- The Customs Criminal Service enrols wanted persons and images of unidentified persons recorded at crime scenes and in the investigation documents.
- The Financial Crime Investigation Service performs the registration of images of unidentified persons recorded at crime scenes and in the investigation documents.

1.3. Habitoscopic Data Register

At the present time, Lithuania has one searchable facial image database. This database is part of an information system that stores information about the appearance of people. It is called the Habitoscopic[26] Data Register (HDR). The custodian of the HDR is the Information Technology and Communications Department, while the data in HDR is owned by the Ministry of Interior. It includes facial images, other habitoscopic data and metadata for individuals who are registered within it. In addition, it includes facial images and other habitoscopic data for individuals who are registered in the database known as the Register of wanted persons, unidentified corpses and unidentified helpless persons (RPSUCUHP), whereas the metadata are stored in RPSUCUHP. HDR and RPSUCUHP are technically integrated such that all the images are stored in one system. Thus, FR searches can be conducted for both registers via HDR.

Facial images in HDR are from suspects, convicts, arrested, wanted persons and persons with unknown identity, in particular:

- Persons who have received the notice about being suspected in performing a crime;
- Persons who under special laws are included into the police register;
- Convicted persons who have been arrested or detained;
- Persons in custody;
- Arrested persons;
- Wanted persons;
- Unidentified dead bodies;
- Helpless persons whose identity is being established;
- Images of unidentified persons recorded at crime scenes and in the investigation documents;
- Persons to whom special screening under the Schengen convention is applied;
- Foreigners detained for illegal trespassing at the state border.

The number of images that can be stored for each person is not limited and the system can contain more than 10 images per person. As of December 2020, there are more than 400 000 facial images stored in HDR, while the number of individuals registered is approximately 185 000.

Facial images of individuals registered in HDR are captured at police stations (detention centres) and at prisons respectively by the police and prison officers. Any digital camera can be used for image capture and the enrolment of images to HDR takes place automatically via the HDR user interface. In addition, in the case of convicts, photographs are captured just

[26] Habitoscopic - habitus (Latin) - the physical characteristics of a person, especially appearance and constitution as related to disease; scopy - viewing or observation (Collins English Dictionary)

before they are released from custody, to ensure that a recent image is included in the database.

Facial images of individuals registered in RPSUCUHP are captured either at police stations or incident locations by police officers using livescan systems and standard digital cameras. Images are automatically enrolled in HDR via the HDR user interface. In the case of missing persons, images are provided by the relatives. If needed, images can also be added from the Population register.

There are no written methods for the capture and enrolment of facial images. However, there are some recommendations – frontal view image looking directly and a yaw angle (left or right), a pitch angle (up or down) and a roll angle (facial tilt) deviation from the direct view should be +/-15 degrees.

All new images are checked automatically by the FR software during the enrolment procedure, which includes an evaluation of the face reliability (i.e. a measure of how confident the system is that part of an image is a face) and face quality (i.e. a measure of confidence that a face is detected). If an image is of poor quality, it is still stored in the database but, is not searchable using the FR module.

The metadata for individuals who are registered in the HDR include name, surname, personal identification number, link to history of criminal records. In addition, the records for some individuals may have a link to other biometric data (i.e. fingerprints and DNA, if such data exists) stored in dedicated databases of the Register of dactyloscopic data and the DNA data register.

Facial images are retained in HDR for a time period as stipulated in the legislation.

Uncontrolled images are not stored in HDR, but in a crime scene register "*Iniciativa*". There is no link between the crime scene register "*Iniciativa*" and the HDR.

1.4. Facial recognition searches

FR searches in HDR are performed by police officers and forensic experts. The searches are conducted with NeoFace Watch v5.1.2 software. An unlimited number of registered users can perform facial searches.

The minimum requirements for the images that are enrolled in HDR, making them suitable for FR searches, are as follows:

- Probe images that are searched against the database images should have at least 20 pixels distance between the eyes;
- Controlled images against which searches are performed should have 80–120 pixels distance between the eyes.

Probe images can be pre-processed for image enhancement purposes, regarding brightness, smoothness, sharpness, cropping and eye correction. This can be done before the enrolment or after the enrolment within the system.

FR search results are candidate lists in which the number of posts can be set by the user. In addition, a score threshold should be set by the user depending on the case situation and the quality of the probe image. All candidates are ranked by a match score (from 1 to 0.01) from the highest match score to the lowest. The higher the score, the more likely it is that the probe image and the candidate image(s) are from the same individual. If the match score is less than 0.55, it indicates that the probe image and candidate image(s) are from different individuals.

FR search results are used for crime prevention, forensic examination and identification. At the present time, the search results are not used as evidence in court.

The FR system has been used for less than one year and thereby there are no annual statistics for the numbers of searches, hits and match rates.

1.5. Quality assurance

There are no written methods for the capture, enrolment and searching of facial images. Nevertheless, the file formats used for the images are JPEG, PNG and BMP. Furthermore, images used for FR should comply with the recommendations provided by the manufacturer of the FR software.

In addition, when FR functionality was implemented in HDR, training was provided by the manufacturer. Altogether, 10 persons have been trained to use the FR search system. However, FR searches can be performed by any police officer. In difficult cases, the police officers that carry out the search can consult with the persons who have received the special training.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

There are two Decrees of the Minister of Interior of the Republic of Lithuania regulating the use of databases and facial images collected in relation to the databases in criminal investigations:

- 21.05.2013 No. 1V-440 “Regulations of the Habitoscopic Data Register”;
- 03.03.2017 No. 1V-174 “Regulations for Register of wanted persons, unknown corpses and unknown helpless persons”.

2. Civil databases

2.1. Population register

The Population register (PR) contains facial images for the permanent and temporary residents to whom an identity document has been issued (i.e. passport, identity card, service passport, diplomatic passport, temporary passport, residence permit, aliens passport, refugees travel document, stateless person travel document applicants). The owner of the PR is the Ministry of Justice and the maintainer is the State Enterprise Centre of Registers.

As of 2020, approximately 3.6 million individuals are registered in PR. One frontal image for each document is stored in the database. According to national legislation, in the event of a change to any data contained in the PR, the new data is entered without deletion of the previous data. The data in PR is retained for an unlimited period.

Alongside an image, the following data is entered and stored in PR:

- Personal code (object identification code);
- Name (names), surname (surnames);
- Gender;
- Date of birth;
- Country and/or place of residence of birth;
- Nationality;
- Citizenship (citizenships), date (dates) for acquisition and deprivation thereof;
- Place of residence (address), date of arrival to the place of residence; if a person leaves abroad to live – place (country) of departure, in case of permanent residence abroad – the state; in case of having no place of residence and is included into the list of persons having no place of residence – municipality of residing;

- Marital status and date of its change;
- Date of death;
- Personal codes of parents, children and spouses; if personal codes are not granted, other personal data which are proved by documents;
- Face image;
- Fingerprints;
- Signature;
- Data of documents;
- Data from the civil status records;
- Data about the incapacity of a person in a certain area or restriction on capacity in a certain area;
- Personal contact data (virtual address (equivalent of the address in virtual environment which recorded in the address register of the republic of Lithuania)); national email address in the information system for delivery of electronic messages and electronic documents to natural persons and legal entities using postal network; fixed or mobile telephone number, if person agrees that his/her phone number is used for the purpose of processing the PR and/or provided to third persons);
- Date of registration of the PR object;
- Date of changing the data of PR object.

The facial data is linked to fingerprints and signature within the PR.

Only administrative data are checked to avoid duplications and respective searches can be performed by personal code or name, surname and date of birth.

The Identity Documents Personalization Centre under the Ministry of Interior performs enrolment of facial images in migration service centres using image capturing stations.

The quality requirements for facial image capture are defined in the Law on the Population Register, Regulations of the Population Register of the Republic of Lithuania, Regulations of the information system of the Population Register. Quality requirements used for capturing facial images are described in ICAO Doc 9303 Machine Readable Travel Documents and in Order of the Minister of the Interior “On approval of photographic requirements for personal documents”.

Currently, FR searches are not possible in the PR. Nevertheless, the data quality within the PR is sufficient to allow FR (and fingerprint) searches, should that be required in the future.

2.2. Register of road vehicle drivers

The Register of road vehicle drivers (RRVD) contains facial images for the applicants of driver’s licences (citizens Lithuania, citizens of other states, stateless persons holding a driving licence issued in Lithuania). The owner of RRVD is the Ministry of Interior and the maintainer is the State Enterprise “Regitra” (REGITRA).

As of 2020, RRVD contains facial images for approximately 1.5 million individuals, one frontal image per driver’s licence. Besides images, RRVD contains driver’s licence information.

Territorial registrars perform the enrolment of facial images or take them from the Population register. Facial images are enrolled in the branches of REGITRA using specially outfitted image capturing stations. Images must comply with the requirements for Photographs for personal documents approved by the Minister of Interior of the Republic of Lithuania 2002 December 6th Order no. 569 (wording of Order No 1V-340 of the Minister of the Interior of the

Republic of Lithuania, 24 August 2006), ICAO 9303 (ver. 6), and ISO / IEC 19794-5: 2011 Photography Guidelines.

It is permissible for RRVD data (including facial images) to be provided to state institutions that need the data to perform their direct functions as established by legal acts (e.g. for criminal intelligence purposes).

At the present time, FR searches are not performed in RRVD.

Luxembourg

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of June 2020, FR has not been implemented in Luxembourg in relation to criminal investigations. Due to a lack of political discussion and legal regulations relating to the use of FR for criminal investigations, there are currently no plans to introduce FR technology. Should a decision to implement this technology be made, the Criminal Police (*Service de Police Judiciaire*) of Grand Ducal Police would lead that work.

At this time, the only database that contains facial images connected to criminal investigation (that, in theory, could be considered for FR) is a database known as the Image Management System (IMS). The custodian of that database is the Grand Ducal Police. There are no concrete plans about making it available for FR purposes.

1.2. IMS database

The IMS database contains images of suspects, convicts and arrestees alongside respective biographic data. On 8 June 2020 the number of individuals registered in this database was 17 790. The database runs on IMS Client software from the PIC Systems.

Images entered into the IMS database include frontal view face, right half-side view face and left side view face along with full body images, and images of tattoos and scars. Should images of the same individual be taken multiple times, all images of that person are retained in the database without any limitation on the number of images that can be stored. Currently, images that are stored are not deleted from the database, however, it is expected that a procedure for data removal will be implemented in the future.

Photographs are taken and enrolled into the database at police stations and administrative offices of the police. Images are captured in custody rooms and penitentiary facilities either by police officers or by other police employees. Digital cameras are used for the photography and the photographs are enrolled in a JPEG format.

During enrolment, the existence of a person in the IMS database is checked on the basis of name and fingerprints as an initial control for potential aliases. This check is performed in an AFIS database and not in the IMS. However, the data in the IMS database is linked to the fingerprint data in AFIS via the AFIS number.

There are no written instructions for the process to capture and enrol images. However, the cameras are set up such that the image dimensions are 4000 x 6000 pixels and the colour depth is 24 bits. In addition, police personnel performing the task receive one-day of training on the job.

The IMS database also contains biographic data: name, alias, gender, date and place of birth, nationality, last known residence address, physical description (e.g. height, eye colour, tattoos etc.) and other remarks.

No uncontrolled images are stored in this database.

2. Legal framework regulating the use of facial images in relation to criminal activity

Collection and use of biometric reference specimens (fingerprints, face and DNA) finds its foundation in the Code of Criminal Procedure. In particular, in articles 39, 45, 47-2 and 51-2 of this law: www.legilux.public.lu/eli/etat/leg/code/procedure_penale/20200320.

Malta

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of October 2019, FR has not been implemented in Malta. This is mainly due to the lack of a relevant legal framework. In addition, Malta currently has no digital facial image databases that could be made easily available for FR in criminal investigations. While the Maltese authorities are aware of the FR technology, there are currently no solid plans to introduce such technology.

2. Civil databases

There are three civilian databases with facial images in Malta:

- National ID card database;
- Passport database;
- Driving licence database.

At the present time, it is not permitted to use the applicant images contained in the above-named databases for law enforcement purposes.

The Netherlands

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

Automated FR has been implemented in The Netherlands since December 2016.

The FR systems of the Dutch National Police are known as CATCH (*Centrale Automatische Technologie voor Herkenning van personen*). Currently, two physically separated CATCH systems are in use: CATCH criminal (CATCH-*StRafrecht*, CATCH-SR) and CATCH alien (CATCH-*Vreemdelingen*, CATCH-VR). The CATCH Alien system data is derived from the core database for foreigners, i.e. *Basis Voorziening Vreemdelingen* (BVV) [Central Register of Foreigners] that, in essence, is a civil database. Searches of the other two largest civil database systems (the municipal identity document registers and the driver's licence database) are permitted in special cases, but currently this is not possible due to technical limitations.

The Dutch Parliament has discussed the use of FR by the National Police and reached the conclusion that the FR implementation to date is legitimate and ethical. However, it has been decided that all future developments in the field must be approved from a legal and ethical point of view.

1.2. Organisations involved

The data in the CATCH criminal is owned by the National Police and the data in the CATCH alien is owned by the Directorate General Immigration (*Directoraat Generaal Migratie*, DGM). The custodian and host of both CATCH systems is the Centre for Biometrics (CvB) of the National Police, who are responsible for the data being used in accord with the legal regulations. In addition, the CvB is responsible for performing FR searches and for the development of the systems.

1.3. Databases of facial images that are used for facial recognition in relation to criminal activity

Legally, it is permitted to use two databases in The Netherlands for FR searches in relation to the detection and prevention of crime:

- CATCH criminal;
- CATCH alien.

1.3.1. CATCH criminal

The CATCH criminal system comprises of an Oracle database and the Face Expert software of Idemia. It contains facial images and a criminal identification number. Related metadata and fingerprints are stored in separate databases and are linked by the unique criminal identification number.

As of September 2019, the CATCH criminal system contains data for 1.3 million persons (annual database growth is about 250 000) and approximately 2.2 million images. These images are taken from:

- Suspects of crimes that are sentenced to 4 or more years imprisonment;
- Suspects of crimes that are sentenced for less than 4 years imprisonment, but whose identity needs to be established (by an order from a public prosecutor);
- Convicts (retention time depending on the type of crime, varying from 20–80 years).

Face and fingerprint data are collected in parallel by police officers or the Royal Military Police using standardized booking stations at 400 police units across The Netherlands. The data acquisition process starts with the recording of personal data (name, social security code etc.), which is followed by the facial image capture and then the final step is the collection of fingerprints. Currently, in the majority of cases, only frontal images are captured, and it is only in rare cases that other views may be taken. However, in the past, frontal images and quarter-view images were obtained.

All acquired data is packaged into a NIST container and sent to the CvB through a web application that has an upload facility. Information from the NIST containers is entered into dedicated databases. Enrolment of facial images is done by trained face experts from CvB. The NIST containers are archived and, if needed, the original data can be retrieved from the archive.

The number of images per person that can be stored is unlimited. The storage time depends on the seriousness of the crime and can be 20, 30 or 80 years. To avoid double identities, the identity of a person is always checked against previous records using fingerprints.

Facial images that are captured from crime scenes (i.e. uncontrolled images) can be searched against the database, but are not stored. However, plans exist to start storing such images in the future.

1.3.2. CATCH alien

The core database for foreigners in The Netherlands is the *Basis Voorziening Vreemdelingen* (BVV) [Central Register of Foreigners]. It contains photographs taken at consulates for Visa or Asylum applications and by police officers or the Royal Military Police using standardised booking stations. A single frontal image is captured and stored together with the capture date and an alien identification number. For each individual whose image is enrolled, other data are also stored: personal data (name, age, gender etc.), legal status (e.g. whether allowed to stay in the country or not) and fingerprints. The identity of a person is checked against previous entries in the databases using fingerprints.

The facial data, an alien identification number and other data about a person from this database are also transferred to the CATCH alien system that is FR searchable. Like the CATCH criminal, the CATCH alien system comprises of an Oracle database and the Face Expert software of Idemia.

The CATCH alien system contains data for approximately 7 million persons. Facial images may be kept in the database for a maximum of 10 years.

1.4. Facial recognition searches

FR searches against the CATCH criminal system and the CATCH alien system are performed at CvB (24/7) by 30 facial experts using a search engine from Idemia. Searches of the CATCH alien system are only permitted with a written order from the public prosecutor and with the consent of an investigative judge.

The searches are performed using probe images with two eyes visible. If needed, images are processed by two persons using the FR software. Currently, the search results are returned as an adjustable candidate list with a maximum number of 50 images. A match threshold is not used. Possible matches are judged by facial comparison experts and handed over to two other facial comparison experts for a second opinion. The result is reported to the police, and sometimes to the immigration services, as an investigational lead only. Whether this information is added to the evidence and presented in a court is decided by the public prosecutor.

In 2018, 1346 search requests were made. In 298 cases, the probe material was of insufficient quality for a search. Of the remainder, 86 (8.2%) resulted in a positive match.

1.5. Quality assurance

The following measures are applied to ensure the quality of images collected from individuals:

- All police officers who take photographs have undergone basic training for the collection of biometric data.
- SOP is in use (*Richtlijn gelaatsfotografie versie* 1.01 13062013), following ISO 19794.
- A standard booking station with a standard camera is in use.

The quality of crime scene images is checked when FR searches are performed. It must be sufficient for making a template and the compliance of the image with the quality requirements of the FR system is checked automatically by the software.

Although the police have no accredited SOP for FR searches using the CATCH systems, the minimum requirements for images to be used for searches are as follows:

- Original file;
- Format: JPEG, BMP or PNG;
- Good sharpness;
- Face-crop;
- Both eyes visible;
- At least 40 pixels between the eyes;
- Maximum pitch and yaw 15 degrees;
- Even lighting;
- Neutral expression.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The most important legal regulations on the use of biometric data, including the use of facial images by the law enforcement agencies are:

- Article 55c in the Law of Criminal Proceedings/Punishment (Dutch Code of Criminal Procedure) stipulating that all pictures taken by the police in offence proceedings can be used for crime prevention, detection, prosecution and conviction;
- Article 107, sub 6, in the Alien Act, stipulating that the use of fingerprints for the detection and prosecution of criminal acts is only allowed if there is suspicion that an alien is involved, investigation is at a dead end or there is urgent need to resolve a case, by written authorization through public prosecutor and investigative judge. Although this law did not foresee the use of automated FR with facial images from aliens, due to the sensitivity of using the biometric data of aliens, it was decided that these rules would also apply for facial images.

2. Civil databases

There are three civil databases in The Netherlands that contain facial images:

- *Basis Voorziening Vreemdelingen* (BVV) [Central Register of Foreigners];
- Municipal identity document registers;
- Driver’s licence database.

In general, it is not permissible to perform FR searches for criminal investigation purposes in the municipal identity document registers nor in the driver’s licence database. However, on special request by the public prosecutor, searches can be performed. Nevertheless, at the present time, FR searches in the civil databases are not technically possible.

1) *Basis Voorziening Vreemdelingen* (BVV) [Central Register of Foreigners]

The *Basis Voorziening Vreemdelingen* (BVV) [Central Register of Foreigners] is considered to be a civil database, however, legally it is permissible to perform FR searches in this register during offence proceedings through the CATCH alien system and this is described above in Section 1.3.2.

2) Municipal identity document registers

Identity documents in The Netherlands are not issued on a national level, instead this is the responsibility of the municipalities. Thus, the municipalities keep registers that contain information, which is collected during the issuing of ID-cards and passports. These registers contain one photograph (frontal only) for each person in the municipality from the last application for a passport or a national ID-card.

Applicants for identity documents provide a photograph in a paper format taken by a professional photographer. The photograph is thereafter scanned by the document officer and entered into the register. Image quality is checked during the interview with the document applicant and the document officers are responsible for ensuring that only good quality images are entered into the database.

In addition to an image, biographic data, a signature and fingerprints are collected. Biographic data (name, date and place of birth etc.) entered in the database is the same for passports and ID-cards. Fingerprints are collected for inclusion within the chip of the passport.

3) Driver's licence database

Rijks Dienst voor het Wegverkeer (RDW) [Department of Road Transport] is the custodian of driver's licence database. The database contains about 20 million images (frontal views only, starting on 1 October 2006) representing about 12 million persons that have applied for a driver's licence in The Netherlands.

The driver's licence application photographs are first processed by the municipality document officers. The applications are then sent to the National Vehicle Authority for the issue of the driver's licence. In the near future, the National Vehicle Authority will start checking the photographs using automated FR to prevent 'doubling' (deduplication check).

Poland

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of February 2020, FR has not been implemented in Poland. This is mainly due to financial, infrastructure and human resource limitations. Furthermore, it was noted that, while demand is on the increase, there is currently insufficient demand for FR systems in Poland. While the Polish authorities are aware of FR, there are no current plans to introduce such technology.

At the present time, facial image examinations in Poland, as performed by the Central Forensic Laboratory of the Polish Police, are restricted to 1:1 comparisons. These primarily consist of analogue images that are digitally scanned and visually compared on computer screens. However, some digital images taken from, for example, video footage are also examined.

Currently, Poland has no digital facial image databases that could easily be made available for FR in relation to criminal investigations. The only database that includes facial images in relation to criminal investigation is known as the *Krajowy System Informacyjny Policji* (KSIP) [Police National Information System]. The organisation responsible for the KSIP is *Biuro Wywiadu i Informacji Kryminalistycznych* [Office of Intelligence and Forensic Information] of the General Police Headquarters of Poland.

The KSIP database contains a wide range of data including images of suspects, individuals that pose a threat to the general public, missing persons, dead bodies, and images acquired during police operations (e.g. CCTV footage and photographs from social media). The quality and format of these images show considerable variation.

The recording of mugshots has been standardised in Poland and facial images are captured from the front and both sides. The majority of mugshots are recorded with the use of equipment developed locally. However, such equipment is not available at all Polish Police stations.

Facial images are held in the database for time periods as stipulated in the legislation.

2. Civil databases

According to the information provided, facial images from various document applications (passports, driving licences etc.) are not stored in digital databases. Applicants for such documents provide a printed photograph which is digitally scanned for inclusion in the relevant document but, the digitised image is not stored on a database. However, the original paper photograph is kept in an analogue archive.

Portugal

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of December 2019, FR has not been implemented in Portugal in relation to criminal investigations. To date, there has been a perceived lack of need for FR even though the legal framework and public perception have not prevented this technology from being implemented. Nevertheless, in recent years there have been a growing number of facial images in various areas of life which has created a practical need to use FR in crime investigations. Therefore, the planning process for introducing the FR technology has started.

At the present time, only 1:1 comparisons of facial images are performed by the Forensic Laboratory of Judiciary Police.

Although, no solid decisions have yet been made for the implementation of FR in Portugal, the most likely scenario is the addition of facial search functionality to the current criminal AFIS and so converting the AFIS system into an ABIS system. This possibility has been under consideration since 2016, when facial images of sufficient quality started to be entered into the criminal AFIS.

1.2. Organisations involved

Forensic Laboratory of Judiciary Police (*Laboratório de Polícia Científica, Polícia Judiciária*) will be responsible for the implementation and use of FR in relation to criminal investigations in Portugal.

1.3. National AFIS databases

It is most likely that the criminal AFIS will be used for FR in Portugal. The current criminal AFIS (version 3.1) is from Idemia and it is owned by the Forensic Laboratory of Judiciary Police.

Both fingerprints and facial images can be stored in the Portuguese criminal AFIS, but at the present time, only fingerprints can be searched. If there is a need to collect fingerprints, facial images are usually taken as well, and both biometrics are enrolled into the AFIS. The systematic collection of facial images with the frontal view image (in accordance with the ICAO standard) was started at 2016. Around 8700 individuals out of 265 000 people registered in AFIS have facial data included in the database. The total number of facial images stored in AFIS (three types of images per individual) is more than 26 000. Front view images meet the quality requirements necessary for FR work.

Biometric data can be entered into the database for a person who has been arrested on suspicion of having committed a criminal offence but, it can be done only after the court has made a relevant decision. In case of an acquittal, information will be removed from the database but, in case of conviction, it is retained in the database for at least 15 years (depending on the type of crime committed). The second reason for entering biometric data into the database is the need to verify the identity of a person but, in such situations, the data must be removed from the database in 30 days.

The following photographs are taken for each person: frontal face image, right side view of the face, left ¾ view of the face, full body image, plus images of special marks, scars and tattoos. These images are all taken without glasses. In case the person wears glasses, additional frontal face and full body images with glasses are taken. From all the photographs that are captured, three views (all without glasses) are entered into AFIS – frontal face image, right side view of the face, left ¾ view of the face. The remaining images will be stored outside of the AFIS database.

Biometric data is collected at police stations all across Portugal, in prisons and in the Forensic Laboratory. Police stations and prisons engaged with the collection of biometry, are usually equipped with the livescan systems for capturing fingerprints and cameras to capture facial and body images. Moreover, data are sometimes collected on paper, i.e. on fingerprint cards. Currently, there are no written instructions in place that regulate how the photographs should be taken. Information obtained during the collection of fingerprints and the capture of facial images by the police and by the prisons is sent to the Forensic Laboratory, where the enrolment of the data into AFIS takes place.

Biometric data is retained in the AFIS together with the reference number of an individual and a criminal case number. All other relevant biographic and criminal case data is stored in the Criminal Investigation Information System. In case the biometric data have been collected multiple times, several sets of fingerprints and facial images per person can be retained in AFIS under the same reference number for the individual.

At the time when FR will be implemented by the Forensic Laboratory, the number of persons working with facial images will need to increase significantly. At the present time, only one fully trained facial expert is engaged with manual 1:1 facial image comparisons and a second person is undergoing training.

Facial images in civil databases that are stored for issuing passports and ID-cards can be used for criminal investigation purposes and are sometimes used for 1:1 comparisons performed by the Forensic Laboratory.

2. Civil databases

2.1. Identity database

The Identity database contains photographs collected for the issue of citizen cards (previously ID cards). The database is owned by the Institute of Registers and Notaries (IRN) that is governed by the Ministry of Justice. It is the largest civilian database of facial images in Portugal.

Citizen cards are issued by IRN and they are a compulsory document for a citizen from 20 days after a birth certificate has been issued. In addition to the citizens of Portugal, Brazilian citizens can also apply for Portuguese citizen cards. There are specific regulations for issuing citizen cards and the management of the Identity database, stipulated in Law no. 7/2007, February 5.

The Identity database contains data for about 25 million individuals (approximately 10 million of them are citizens of Portugal living in Portugal, 5 million are citizens of Portugal not living in Portugal and 10 million are Brazilian citizens).

It is compulsory to attend an issuing authority (IRN) during the first application for a citizen card. Thereafter, citizen cards must be renewed every five years and this can be done online. Facial images can be taken and enrolled to the central database in many places (204 local offices in Portugal and 124 offices all over the world in Portuguese embassies). Special workstations (Vision-Box'es) are used for the capture of facial images and the collection of fingerprints in IRN offices. Mobile devices are used if a person cannot attend the office and also in hospitals (e.g. for taking the pictures of new-born babies). In addition, digital images submitted by the applicants are also acceptable.

One frontal view image and two fingerprints (index fingers) are collected for the issue of a citizen card. Photographs are taken according to the ICAO standard and are stored in a JPEG format. All IRN agents working with capturing devices in Portugal have undergone 15 days of training. E-learning is provided for persons working abroad. Also, a mentoring system is used. For the data collection, written procedures are in place.

The facial image and the fingerprints are stored on the chip of the card, in the Identity database and accordingly, in the civil AFIS. Non-biometric data that is stored in the Identity database include: name, civil ID number, date of birth, gender, nationality, height, parents, home address, signature, date of issue and expiry. The Identity database, where the photograph and non-biometric information is stored, is linked with the civil AFIS and with the birth certificate database. The identity database is not searchable by facial images, but a search can be performed with fingerprints using the civil AFIS and this is done regularly for verification purposes.

All the images that are taken of a person can be stored in the database. Images are deleted 20 years after the death of the person.

Law enforcement agencies are permitted to ask for a photograph from the Identity database for 1:1 comparisons. This is regulated by Law no. 33/99, May 18, Articles 24º to 27º. In addition, the police are working on a technical solution that would enable fingerprint searches within the civil AFIS for verification purposes but would prevent searches of the civil AFIS using latent prints.

One of the additional responsibilities of IRN is the collection of facial images for passports. However, passports are issued by the Ministry of Foreign Affairs and, accordingly, passport photographs are also retained by the Ministry of Foreign Affairs. Since the same equipment, standards and procedures are used by the same persons capturing images for citizen cards, all the previously described technical details are also valid for the passport images.

2.2. National registry of drivers

The National registry of drivers contains personal information and photographs for people authorized to drive any vehicle, ranging from cars to trains. The register is kept by the Institute of Mobility and Transportation (IMT) under the Ministry of Infrastructure and Housing. In addition to keeping the registry of drivers, IMT is also responsible for keeping the registration certificates of vehicles. Legally, the collection and storage of facial images in the register is regulated by Decree-Law no. 262/2009, September 28, as amended by Decree-Law no. 12/2017, January 19.

There are more than 7 million individuals entered into the National registry of drivers. Currently, facial images in the National registry of drivers are either derived from the Identity database or are captured at the desk service of IMT. The submission of photographs by the applicant is not allowed. Any person holding a driving licence issued in Portugal (regardless of his/her nationality) may use the online services (www.imtonline.pt) to apply for the renewal or replacement of his/her driving licence. In such a situation, the applicant grants IMT permission to either use a previous photograph in the register or to download an image together with a signature from the Identity database. There are 21 local IMT desk services all over mainland Portugal equipped with webcams where photographs can be captured. Written instructions for capturing images have been developed for personnel taking the images. Furthermore, in-house training is provided.

Only frontal view images in JPEG format are entered into the database, although TIFF format images have also been used in the past. The quality of the image is checked by the database software automatically. In addition, if the application is not submitted online, but in the office of IMT, the image quality is checked by the employee of IMT.

All images of a person that are enrolled are stored in the database, but only the last one is used for issuing the driver’s licence. No rules have been set for the deletion of images from the register.

Alongside photographs, the register contains the following information: name of the person, civil ID number, gender, date and place of birth, nationality, signature, number of the issued document etc.

Police are permitted to ask for a facial image from the National registry of drivers, but this is rare since, in many instances, the source of a facial image is another register (the Identity database).

Romania

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of November 2020, FR for the investigation of crime has not been implemented in Romania. However, work towards introducing FR technology within the Romanian Police is currently ongoing. A tender for acquiring a FR system has been successfully finalised and, at the present moment, the Romanian Police is engaged in the implementation process for the system. The system is expected to become operational at the end of April 2021.

In addition, a national facial image database (National Biometric Identification System) has been developed and prepared for FR search purposes by the Romanian Police. As of November 2019, the database holds images from approximately 300 000 individuals and this will increase by more than 500 000 individuals after being populated with data from an old facial image database in police use, known as Imagetrak.

Currently, manual 1:1 comparisons of facial images are performed by the National Forensic Institute of the Romanian Police. For such comparisons, the police are permitted to use photographs from civilian applications.

1.2. Organisations involved

The National Forensic Institute of the Romanian Police is responsible for the implementation of FR. Technically, the implementation steps are also being supported by the General Directorate for IT of the Ministry of Internal Affairs and the Directorate for IT of the General Inspectorate of the Romanian Police. The Romanian Police are the owner and the custodian of the National Biometric Identification System (NBIS).

1.3. NBIS

Romania has planned a single national facial image database for use with FR searches in criminal investigations. This database is NBIS owned by the Romanian Police. NBIS went into production in September 2016 and has been developed in-house.

In November 2019, NBIS contained images from approximately 300 000 individuals. However, images from more than 500 000 individuals from an old non-operational facial image database (Imagetrak) are yet to be transferred to NBIS. The Imagetrak database is also owned by the Romanian Police.

Images in the NBIS database include those taken from suspects and convicts. In addition, the database contains images of unknown persons (i.e. persons whose identity has not yet been established), missing persons and unidentified dead bodies.

As a rule, each individual who is registered in NBIS has one record. During the registration process of a new individual whose identity has been established, a personal identification number is used in order to check whether the person has any prior records in NBIS. If the person has an existing record, that record is updated instead of creating a new one. Duplicate records of the same person (e.g. that might arise during the transfer of images from Imagetrak to NBIS) will be merged. In the case of unknown individuals, an identity is established either by using fingerprints or DNA. If it is not possible to establish the identity of an individual, he/she will be registered as an unknown person.

The database records may contain an unlimited number of images per person. Typically, the following images are taken and enrolled in the database:

- Front view facial image;
- Side view facial images from right and left;
- Full body photograph (frontal view);
- Images of special marks, scars and tattoos.

Images are taken and enrolled into NBIS by forensic examiners of the Romanian Police at police stations in 41 counties, at one police station in Bucharest and at the National Forensic Institute. A request for capturing an image is submitted by police officers and investigators. Depending on the request, a facial image or a facial image together with other biometrics (i.e. fingerprints and DNA) can be collected. Photographs are taken using digital cameras but there are plans to replace these with livescan capturing stations in the future.

The minimum resolution requirement for images is 1024 x 768 pixels. Images in NBIS are in PNG format, while images in Imagetrak are in JPEG format. No compression is applied to the PNG images, but a standard JPEG compression is used for images in that format.

Alongside the images, biographic data (e.g. name, addresses, name of parents), reason for photographing a person, and a criminal record number (if one exists) are stored in NBIS. The biographic data of Romanian citizens can be extracted from the Persons Records Database into NBIS by using a unique personal identification number. Other biometric data (i.e. fingerprints and DNA) collected from the person are stored in separate dedicated databases that are not directly linked to NBIS. However, information about the availability of other biometrics is indicated in NBIS.

Facial images are retained in the database for time periods as stipulated in the legislation. Data can be deleted on the basis of requests from courts, investigators and prosecutors.

At this time, uncontrolled images are not stored in NBIS. However, there are plans to store such images in NBIS in the future.

1.4. Facial recognition searches

Forensic examiners of the Romanian Police, who are specialized in facial image examinations, will be trained to perform FR searches after the implementation of the FR system. NeoFace Watch software from NEC has been acquired for this work and is currently being implemented.

Although FR searches are not being performed at the present time, the initial requirements for the search capability have been established. For FR purposes, only frontal face images will be used. Probe images must have at least 20 pixels between the pupils and, ideally, FR users will have the possibility to pre-process a probe image by cropping and/or enhancement. A threshold for a candidate list will be set by the user depending on the specific case, but no “lights out” scenario is planned for the implementation.

FR search results will only be used as a lead in criminal investigations and will not be used as evidence in the court. For court purposes, only the results of 1:1 comparisons will be eligible when presented as expert reports.

1.5. Quality assurance

Facial images are captured according to ICAO 19303 and ISO 19794 standards. In addition, an internal SOP has been developed for the capture and enrolment of images. The SOP has been distributed to all police stations across Romania and describes the quality requirements for lighting conditions, format, pose etc., and for the additional information that needs to be entered in NBIS alongside the images.

Furthermore, training is provided to forensic examiners who capture and enrol images. This is delivered by experts from the National Forensic Institute of the Romanian Police.

Regarding ISO 17025/2018 accreditation, as of November 2020, the National Forensic Institute of the Romanian Police has obtained a multi-site accreditation for biometric examination, including facial examination through NBIS and Imagetrak.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The most important legislative act is Law No. 218/2002 for the Organization and Functioning of the Romanian Police (http://legislatie.just.ro/Public/DetaliiDocument/35841), which allows the police to collect data (including biometric data such as fingerprints, DNA and facial images), store the information in databases, and use it for crime investigation, detection and prevention. This law is not specific to biometric data but, regulates various areas of police activity.

2. Civil databases

Facial images for civilian use are collected and stored in the following databases:

- Immigrants database owned by the General Inspectorate for Immigration;
- Passport, ID Card and Driving Licence databases owned by the Ministry of Internal Affairs.

Slovakia

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of October 2019, FR has not been implemented in Slovakia. This is mainly due to a lack of finance and a low demand for a FR system. Another reason for the non-implementation of FR technology is the general opinion of the Slovakian authorities that fingerprints are much more reliable than facial images. However, there is an interest within the Presidium of the Police Force and the Institute of Forensic Science to introduce this technology in relation to criminal investigations. Should facial recgnition be implmented in the future, the Ministry of Interior will be responsible for this work.

Facial images are collected and stored by the Slovakian Police in several databases. However, no concrete decisions exist about making any of these available for FR purposes at the present time.

Police officers of the Presidium of the Police Force have access to images stored in the civil databases for ID-cards, passports and driving licences. The use of such images in criminal investigations is allowed for manual 1:1 comparisons with permission from a judge. This work is performed by the Institute of Forensic Science of the Presidium of the Police Force.

1.2. Police databases that contain facial images

1.2.1. AFIS

Only one AFIS exists within the Slovakian Police. The AFIS is used for different applications, such as criminal investigations and border control. The system runs on software from Cogent. The custodian of the AFIS system is the Institute of Forensic Science, whereas the owner of the data in AFIS is the Ministry of Interior.

AFIS has two sub-systems that are logically separated – Criminal AFIS and Foreigners AFIS.

Criminal AFIS contains data from:

- Slovakian citizens – fingerprints and biography, from June 2020 it may contain facial images.
- Third county nationals or EU nationals detained, accused, or convicted in the Slovak Republic territory – fingerprints and biography, from June 2020 it should contain facial images (mandatory for ECRIS-TCN application).

Foreigners AFIS contains data from:

- Third country nationals crossing the Slovakian border from whom data collection is not connected to criminal activity – facial images, fingerprints, and biography. Although not initially taken for criminal investigation purposes, the law allows the use of facial images and fingerprints for the investigation of crime. Data from this group of persons is collected by the Border Police. The same data is also stored in a database known as MIGRA.

The Criminal AFIS holds fingerprints from 350 000 individuals and the Foreigners AFIS holds fingerprints and facial images from 150 000 individuals.

As the current facial images in AFIS are mainly related to border crossing, the following information describes the data collection at borders.

The facial images in AFIS date back to 1995. As facial data have been collected for 25 years, the image types, image quality and format vary considerably. Before 1996, facial images could have been taken from different angles and sometimes a frontal face image may not have been captured. In 1996, the first standards were introduced and the capture of a frontal view face image became a mandatory requirement. From 2004, in connection with Eurodac Regulations, the facial image quality was improved significantly, with manuals and training programmes being developed and implemented. Facial images are captured using digital cameras. Standardised equipment has been used since 2004 at all border crossing points within the Schengen area. Enrolment takes place automatically. Accepted file formats for facial images are JPEG, BMP and TIFF with images being compressed.

The biographic data entered in AFIS include full name, aliases, nationality, passport number, date of fingerprint and image capture, place where biometrics were taken, and a scanned copy of an identification document. Facial images and fingerprints are linked within the system and all data are stored indefinitely.

A search capability is currently only available for fingerprints, however, the system is ready for an upgrade to include FR search functionality. This makes AFIS one of the candidate databases to be used for FR.

1.2.2. IPOLDAT

IPOLDAT (Police Information Database) contains the facial images of criminal offenders, the majority having been convicted. The custodian of the database is the Presidium of the Police Force and it is owned by the Ministry of Interior. As of October 2019, approximately 500 000 individuals were registered in IPOLDAT.

The facial images of the persons stored in IPOLDAT are taken from the front, right side and left ¾ side at police stations across the country. Police officers who capture and enrol images into the database use digital cameras, which vary in different police stations. The file format used is JPEG.

According to a sub-law of the Ministry of Interior, images are retained in the database until the death of a person (maximum 100 years from entry into the database).

Biographic data is stored alongside images, including full name, date of birth, residence address, and name of parents.

In theory, images in IPOLDAT could be used for FR, however, the database itself is too old to be upgraded for this purpose.

1.2.3. PATROS

PATROS (*Pátranie Osoby*, in Eng. Searching for Persons) contains personal data, including photographs, of wanted persons, missing persons and unidentified dead bodies. The custodian of PATROS is the Presidium of the Police Force and it is owned by the Ministry of Interior.

The photographs that are stored in PATROS are either automatically obtained from the Registry of population (REGOB) or entered manually. For instance, in the case of a missing person, the most recent photograph is sometimes provided by the relatives. Depending on the source, the photographs in PATROS are of different quality and format. Nevertheless, in theory, this database could be considered suitable for FR purposes.

2. Civil databases

There are five major civil databases in Slovakia that contain facial images:

- Registry of population (REGOB);
- ID-cards database;
- Passports database;
- Database of driving licences;
- Database on foreigners (MIGRA).

The information below describes the databases for ID-cards, passports and driving licences. Images from these databases are also transferred to, and stored in, REGOB. Furthermore, images from REGOB can be transferred to PATROS if required. MIGRA is addressed in section 1.2.1. in relation to the Foreigners AFIS.

Altogether, 7 million images have been collected from the applicants of passports, driving licences and ID-cards (a mandatory document for Slovakian citizens from 15 years of age with a permanent residence in Slovakia). For these documents, frontal face images are captured (in accord with the ICAO standard) within regional departments of Documents and Records of the Slovakian Police. Photographs are captured by officials from these departments using special capturing stations with digital cameras. During the application submission process, these officials will check the identity of the person against previous documents (if they exist) and enrol photographs (JPEG format) into the system. The system software performs a quality check of the image and compares it against any previous image for the person. Document renewal can be done online in situations where the latest image stored in the system is not older than 5 years. All images taken of a person in the document application processes are retained in the database and there is no limit to the number of images that can be stored.

Alongside the images, biographic data is also stored and this varies according to the type of document. Common biographic data in all document applications include full name, personal identification number, date of birth, residence address, and ID number.

Other biometrics (i.e. fingerprints) are only collected for biometric passport applications. Whilst the fingerprint data is deleted after the passport has been issued, photographs and biographic data are stored permanently.

Police officers have access to the database images for ID-cards, passports and driving licences, and these can be used for 1:1 comparisons. Nevertheless, police officers cannot make any changes within these databases.

Slovenia

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

Automated FR in Slovenia was introduced for criminal investigations in 2015.

The Record of photographed persons owned by the Slovenian Police, is the only database used for FR. It contains photographs collected from suspects, missing persons, and unidentified dead bodies. As of November 2020, the number of individuals with images in the database is about 110 000. In addition, the database contains images made with photo robot and, from November 2020, uncontrolled images are also included. FR searches are performed by 15 police officers at the regional level and by 2 police officers at the state level. The search results can be used only for investigative purposes. For court, manual 1:1 facial image comparisons must be performed, with the results presented in appropriate reports. These comparisons are conducted by the same 2 police officers who carry out the FR searches at the state level.

It is permissible, for the images in civil databases (from applicants for passports and identity cards) to be accessed by the police during criminal investigations, but the civil databases are not FR searchable.

1.2. Organisations involved

The General Police Directorate of the Slovenian Police is responsible for the following:

- Implementation and development of FR;
- Database used for FR;
- Capture and enrolment of facial images;
- Submission of search requests;
- Performance of searches and evaluation of search results.

1.3. Record of photographed persons

According to the law (named the Police Tasks and Powers Act) the Record of photographed persons is one of the databases used by the Slovenian Police. It is the only database used by the police for FR. The database management uses Face Trace software from Neurotechnology.

The following images are included in the database:

- Photographs of suspects;
- Photographs of missing persons;
- Photographs of unidentified dead bodies;
- Images made with a photo robot (about 100 images).

Recently (from November 2020), uncontrolled images (e.g. images obtained from surveillance cameras) are entered and stored in the Record of photographed persons.

Since 2007, the photographs entered into the database have been taken in a digital format. Images in an analogue format that were taken before 2007, are scanned and entered to the database, if needed.

The following images are taken from suspects for databasing purpose:

- Front view facial image;

- Right side view facial image;
- Left half-side view facial image;
- Images of tattoos.

Only frontal view facial images can currently be searched using the FR tool.

Photographs are taken and enrolled into the database by criminal technicians (approximately 75) in 8 regional units of the police. In addition, there are 2 police stations where all police officers can perform these tasks. Firstly, the identity of the person is established, which is primarily done by a document check and via fingerprints using the criminal AFIS database. Next, the images are captured using digital cameras (either 50 mm lens or 36 mm lens) and images are enrolled into the database. The file format used for the images is JPEG (maximum 800 kB) and the image resolution is 300 PPI.

During the enrolment process, biographic data of the person is entered in the Record of criminal offences (i.e. record for criminal case data). A unique code is generated and, through this code, the biographic data is linked to the images of that person in the Record of photographed persons.

In addition to the images, the Record of photographed persons contains alias/false name, a description of the person (e.g. height, constitution, skin, hair and eye colour, face shape, characterization of forehead, nose, ears, hair, facial hair and teeth, wearing of glasses, special marks/tattoos), the place, time and reason for taking the photograph being taken, and the full name of the person who took the photograph.

As of November 2020, the database contains images from about 110 000 individuals. If an image of the same person is enrolled several times, all images are retained in the database. Thus, multiple images per person may be held.

Photographs are deleted from the database within 45 days after the police are informed about the end of criminal proceeding when a person is not convicted. If a person is convicted, the time period for retaining the photographs in the database depend on the seriousness of the crime committed. This time period can be between 8 and 50 years.

The Record of photographed persons does not have a direct link to other biometric databases, since all three databases (facial, DNA and fingerprints) are processed separately.

1.4. Facial recognition searches

The FR searches are performed using VeriLook from Neurotechnology. This work is done by 15 police officers at the regional level and by 2 police officers at the state level.

For FR searches, probe images must meet a minimum criterion of having 150 pixels distance between the eyes. As a result of the search, a candidate list of 51 posts is received. The candidate list is evaluated by the person performing the search and a decision is made about whether there is a “match” or not (based on the experience of each individual police officer). Search results are reported to investigators and are used as an investigative lead. In order to use the search result as evidence in court, a manual 1:1 comparison must be performed and a relevant report prepared. The manual 1:1 comparisons and the court reports are done by the same two people who perform FR searches at a state level.

Approximately 150–200 searches are performed each year and 2–3 hits are obtained. Thus, the current match rate is around 1%.

1.5. Quality assurance

The quality aspect of FR work is regulated by the following documents:

- Procedure for photographing of suspects;
- Enrolment of images;
- Using of Face Trace module and performing FR searches.

No special training is provided for the individuals who enrol facial images and perform FR searches. Instead, they receive in-house training via a mentoring system.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

Legislative acts that regulate the use of biometric data, including the use of facial images by the law enforcement agencies are the following:

- Police Tasks and Powers Act – the most important act regulating the collection and processing of biometric data by the police;
- Criminal Procedure Act – an act stipulating that facial images can be taken from suspects;
- Personal Data Protection Act – an act regulating the general principles how personal data must be used and to which the above-listed legislative acts must be in accordance with.

2. Civil databases

Slovenian citizens with a permanent residence in Slovenia who have reached 18 years of age, must have at least one identity document from the following list:

- ID-card;
- Travel document (passport, border crossing pass);
- Driving licence;
- Permit to drive boats;
- Arms permit.

All the above-named documents are issued by the public authorities of Slovenia and include a frontal view image of the person.

Similarly, an identity document that is issued to foreign nationals by their country of origin is obligatory for all non-citizens who reside in Slovenia. In addition, such individuals have residence permits issued to them by Slovenia.

Regarding different types of identity documents, the following databases are maintained:

- Record of ID-cards;
- Record of passports;
- Record of driving licences;
- Record of temporary residence permits, permanent residence permits, visas and passports for aliens.

All these records are managed by the Ministry of Interior with the exception of the Record of driving licences which is managed by the Ministry of Infrastructure.

As of December 2019, the number of ID-card holders is more than 1.8 million, the number of valid travel document holders is about 670 000 and the number of driving licences is more than 800 000. Facial images are held in the Record of ID-cards from 1998 and in the Record of travel documents from 1991.

Photographs for identity document applications may be submitted either in a physical or digital format. Only e-photographers licenced by the Ministry of Interior are mandated to take digital images using specialized software. The number of such photographers in Slovenia is more than 100.

A specially equipped image capturing station called a High-Performance Workspace (HPW) is used for capturing facial images by the authority where document applications are submitted. HPW consists of a web application for capturing biometric data and peripheral equipment such as high-resolution image scanner, a fingerprint reader and a signature plate. The web application allows quick access to information about registered persons and serves for record photographs, fingerprints and signatures. At the same time, it checks the compliance of the captured data with international standards such as:

- ICAO 9303 7th Edition 2015;
- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents;
- ISO / IEC 19794-5: 2005: Biometric data exchange formats - Part 5: Facial image data.

Paper photographs (3.5 x 4.5 cm) are also checked for quality, according to the international standards named above and scanned by the authorized person for enrolment purposes.

The enrolment of facial images is performed by the employees of administrative units (58 across the Republic of Slovenia), employees of the Ministry of Interior of the Republic of Slovenia and employees of the diplomatic missions or consulates (50 of the Republic of Slovenia abroad). In total there are about 400 enrolment points.

Alongside facial images other information is stored in the database: personal data such as name, surname, gender, date of birth, citizenship, permanent residence and signature, and data on the issued document such as document registration number, serial number, application submission date, document production and issue to applicant date. Personal data on individuals are transferred to the above-listed records from two other registers – the Register of civil status and the Permanent population register.

The records relating to identity documents, hold the history of valid and non-valid documents (including the history of the images stored for a given person). The data from a specific document application are retained for 5 years after the expiry of the issued document. After that, the data is archived permanently.

Fingerprints are collected from the applicants for passports from 12 years of age. Collected fingerprints are stored in the records until the document has been issued. The fingerprints are also stored in the electronic chip of the document.

The most important legal acts regulating the field of civil databases are:

- Identity Card Act;
- Rules on the Implementation of the Identity Card Act;
- Travel Documents Act;
- Rules on the Implementation of the Travel Documents Act;
- Drivers Act;
- Rules on Driving Licences.

It is permissible for photographs collected for the issue of identity cards and passports to be accessed by the police during criminal investigations. None of the civil database have FR search functionality.

Spain

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of October 2019, FR searches against the mugshot database have not yet become operational in Spain, although FR technology is already being used by the police for research and development, and intelligence purposes.

The FR system from Thales was purchased in 2019, after about five years of testing and negotiations between the different police forces in Spain, who all will share a centralized system. The face modality will be added to the current Thales AFIS system and, thereby, AFIS will be converted into an ABIS system. Originally, it was estimated that the ABIS implementation would take place during 2020, however, it has been delayed as a side-effect of the unforeseen COVID-19 outbreak.

There are several separate mugshot databases in Spain. The National Police handles a large national mugshot database, but there are also smaller mugshot databases handled by the Civil Guard and the Regional Police forces. Altogether, these databases hold 5.6 million images for 3.9 million individuals. All units that own mugshot data will send copies of their images to the ABIS system. The FR searches will be performed in this centralized ABIS database. Since the ABIS system has yet to be implemented, the technical details and solutions are yet to be specified. The Ministry of Interior is responsible for the implementation of the ABIS and the FR system. The searches will be done by ABIS operators at the forensic departments of the different police forces and there is planning being developed for workflow harmonization between the different police forces. The plan is to use the search results (potential candidate reports) as investigative leads and not for court use.

Currently, there are no plans to implement FR searches against any other databases in Spain. However, the police can request facial images from civil databases for 1:1 comparisons, but not for use with FR searches.

1.2. Organisations involved

Ministry of Interior (*Secretaría de Estado de Seguridad*): owner and implementer of ABIS, owner and implementer of the FR system.

National Police (national): FR users, forensic face examiners, mugshot database owner.

Civil Guard (national, rural areas): FR users, mugshot database owner.

Regional Police (countryside): FR users, mugshot database owner.

1.3. Databases of facial images that will be used for facial recognition in relation to criminal activity

The plan is to include all the digital images from the separate mugshot databases (developed in-house) across Spain into a centralized ABIS system with a FR engine. It is likely that old analogue images will not be included in the ABIS system.

In total, the mugshot databases include 5.6 million images of 3.9 million individuals (as of November 2019). About 4 million of these images are legally owned by the National Police, and the rest by the Civil Guard and the different Regional Police forces. The separate mugshot databases across the country are all connected, making it possible to consult directly with all the police force databases. The exception is the Basque county database that is not connected to any other local databases.

Mugshot photographs are taken at the police stations when a person is arrested. The mugshot is always collected together with fingerprints, and with DNA in the case of serious crimes. When a person is arrested, the person's identity is always verified against the National ID database using fingerprints. If the given identity turns out to be false, the new entry in the mugshot database is linked to the identity of the matching fingerprint ID.

The databases contain images of frontal face, right and left profile, semi-left profile (some districts also have semi-right profile), full body frontal, and marks, scars or tattoos. For the FR system, the frontal image will be used, and possibly, the semi profile image. The minimum image size and resolution requirements are 2 Mb and at least 300 PPI, respectively. The images are of JPEG format, and the compression is selected according to the available JPEG camera settings.

The metadata connected to the mugshot images contain: name, nickname, national ID, whether the identity was checked by index fingerprints against the National ID database, date of birth, place of birth, name of father, name of mother, gender, stature, mugshot ID, picture number, alerts if the person is considered to be dangerous, have used any weapons, was arrested together with other criminals etc. A few of these data fields are searchable (e.g. name) but most are not (including biometric descriptions, such as hair colour).

There is no limit in the mugshot databases to the number of facial images that can be taken and stored for a given individual. Once the time limit for storage of the image has passed, the individual can ask to have the data deleted from the database. If such a request is not received, the data can be stored in the mugshot database for an unlimited time period.

1.4. Facial recognition searches

The purchase of the FR system was finalised recently (2019). The search engine will be from Thales, the same vendor as the fingerprint and ABIS systems. Since the ABIS system is not yet fully implemented, Spanish police organisations are currently not doing any FR searches against the mugshot database. However, work on the implementation is underway, and therefore the information in this section is tentative and preliminary, as many of these issues will be determined at a later stage.

The FR search operations were expected to start during 2020, but this has been delayed. The idea is that all the data in the separate mugshot databases will be automatically synchronised with the ABIS system. Also, the option to have a logical separation between the mugshot database and uncontrolled images database might be considered in the future.

The workflow has not been fully decided yet, but it is anticipated that it will be similar to the workflow used for fingerprints. Most likely, the searches will be performed by persons on the competence level of reviewers, meaning persons who use the ABIS system for biometric searches and analyse the candidate lists. At the National Police, there will be about 350 user licences, the same as for fingerprint AFIS users. Primarily, it will be the forensic face examiners who will perform the searches, but it is possible that fingerprint examiners may also perform FR searches, depending on the work demand.

Before the start of FR operations, the caseloads are unclear, and decisions will be required as to whether there will be any restrictions on when searches will be allowed (e.g. type of crime, image quality). Depending on the workload, restrictions for volume crime may be implemented, but such restrictions are not expected for serious crime.

As to the possible pre-processing of probe images, the current view is that restrictions will not be necessary because the results will only be used for intelligence purposes and not for court reporting. For example, all police stations have access to Adobe Photoshop. Nevertheless, with the new FR algorithms, it is not believed that image pre-processing will significantly improve the search results.

It has not been decided whether any threshold will be used for the search results and, further, decisions are outstanding as to the number of candidates that will appear in the search output. Moreover, the possible implementation of a "lights out" scenario has not yet been discussed and this will depend on the future workload and other factors.

The search results will be manually analysed by a reviewer who will observe similarities and dissimilarities when considering whether a candidate could be the same person in the probe image, or not. The results will be reported as investigative leads, probably as "potential candidates", and this will act as intelligence for the investigator to follow up. The report will be very basic, and is not for court use. If the images are to be used in court, a forensic 1:1 facial image comparison must be requested.

1.5. Quality assurance

Mugshot data is acquired at police stations by police officers from the forensic units. They are specifically trained with a one-month training program, of which, one week is specific training for mugshot capture. There is also a written manual to follow and a course on enrolment in the system.

There is no specific standard for facial image acquisition, but the images are captured under homogenous and specified conditions, resulting in very good quality images. All police forces use the same camera equipment and background settings (black). Some police stations also have a chair which can rotate to take the profile pictures. Thus, images in the mugshot database have been found to be of homogenous data quality, even though there is no automatic quality control at the capture stage. Currently, there are no plan to implement any international standard for image quality.

1.6. Legal framework regulating the use of facial images in relation to criminal activity

In Spain, the general rules on criminal law are contained in the Penal Code (Organic Law 10/1995, 23 November) and the Law on Criminal Procedure (approved by the Royal Decree of 14 September 1882). The legislative acts that regulate the use of biometric data by law enforcement agencies, including the use of facial images, are described as follows:

- Organic Law 15/1999 of 13 December on the Protection of Personal Data, Article 22. This law covers the regulation of the usage of personal data in criminal procedures. In principle this law is not active anymore, except Article 22 that is still active. The law is currently under transition due to the European GDPR directive (transposing Directive 2016/680).
- Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. This is the transition law on data protection and digital guarantees that allow Article 22 still to be active during the transition into a new law.

The face biometric modality is governed by the same regulations as the fingerprint and DNA modalities, and therefore no legal alterations are anticipated for implementing FR searches against the mugshot database.

2. Other databases related to criminal activity that contain facial images

1) Persons of interest (uncontrolled images)

Unidentified offenders captured on imagery, such as CCTV or fake documents, are stored in a database at the investigation unit of the National Police. There are about 50 000 images in this database, but there might also be similar smaller databases in regional police forces. Currently, there is no plan to include the database of uncontrolled images into the FR system. However, there are plans to search these images against the database.

Metadata connected to the uncontrolled images include: case number, investigating unit, date of crime, place, type of crime, modus operandi, weapons (gun, knife etc.), itinerary (travel route) and written descriptions of the perpetrator (from the image).

The requirements for the uncontrolled images are that they must be in a JPEG or PNG format, have a maximum size of 400 kB, and contain only the face of the person.

There is no time limit as to how long the data is retained (there are no specific time rules). For severe crimes, images are usually retained for a longer time period than for less severe crimes.

2) Prison images

The prison image database is owned by the Ministry of Interior. There are no plans to include these images in the ABIS, since all the people in prison already appear in the mugshot databases. Also, these images are of lesser quality than the mugshot images.

3. Civil databases

There are two major civil databases in Spain that contain facial images:

- National ID
- Passport databases

The National Police, Documentation Division, are the owner and the manager of both the National ID card and Passport databases. There are around 67 million persons registered in the National ID card database. However, this number also includes deceased persons and there is no upper time limit as to how long records can be retained in the database. No data is available for the number of persons registered in the Passport database.

A maximum of three images for each person are saved in the National ID card database (the three latest images) and seven in the Passport database. Only frontal images are enrolled in these databases, where the head should be uncovered (exceptions are possible for religious reasons), eyes open and if a person wears glasses they should be translucent. Blind people are allowed to use dark glasses. According to Royal Decree 1553/2005 regulating the issuance of the ID card, the image must be recent, in colour with a uniform white and smooth background, and in a size of 32 x 26 mm.

Images for the ID card are submitted by the document applicant on paper and scanned for entering into the database. For passports, there are two options. If the person has a valid ID card not older than 2 years, the image is automatically transferred from the National ID card database to the Passport database and the applicant can have this image used for the issue of the passport document. Alternatively, the applicant can provide a new photograph on paper. Metadata stored in the databases alongside images include: name, surname, place and date of birth and parent's names. For ID cards, a residence address is also included.

The administrative data are provided by the citizen at the time of the first document application. This is done through the presentation of a birth certificate to the issuing authority. In case of document renewal, a comparison is made with the fingerprints in the existing document, so that there is no risk of double records. However, facial images are not checked during a new enrolment, because the image is currently scanned from a physical image provided by the citizen. In the near future, it is anticipated that facial images will be captured by a webcam. When the citizen wants to change some data, they must first request it in the corresponding Civil Registry, and once that change has been granted, they need to request that the data in the document are changed, accordingly. This change will only be carried out after a verification by the Documentation Division, ensuring that it is the same person.

FR searches are not performed in the National ID nor in the Passport databases. In principle, such searches could be allowed, if the owner of the images express his or her explicit consent, or when he/she is in any of the situations set out in Regulation (EU) 2016/679. However, currently, the biometric data contained in the database can only be used in criminal investigations when required by the judicial authority, individually and without being able to carry out mass searches of this data.

Due to the limitations imposed by Regulation (EU) 2016/679, and Spanish Law 3/2018 on the Protection of Personal Data, it would be difficult for biometric data in the National ID card and Passport databases to be included in search programs for criminal purposes in the future. However, a project is being promoted for the creation of a computer program that would allow the automatic searching of fingerprints for civil purposes (i.e. searching the information held in the databases of ID cards and Passports). The civil purposes include the identification of missing persons and unidentified corpses, people in vulnerable situations and major disaster situations. There is no comparable project in terms of facial images.

Sweden

1. Facial recognition in relation to criminal activity

1.1. Summary of current situation

As of November 2020, the implementation of FR in offence proceedings is underway and is expected to be finalised sometime during 2021. Once implemented, the National Forensic Centre (NFC), part of the Swedish Police Authority, will have the capability to search facial images against the national mugshot database. The database was digitised in 2014, and currently contains around 60 000 entries, with a yearly increase of approximately 10 000.

During the spring of 2019, a pilot of searching real criminal case facial images against the mugshot database was conducted by the NFC. The outcome was very successful, with a potential candidate reported in roughly every fourth case. Prior to this, the procedure of using a FR engine to search the mugshot database underwent a legal analysis at the legal department of the Police authority, followed by a consultation with the Swedish Data Protection Authority (DPA). The outcome of the DPA consultation was that they agree with the previous legal analysis in that the planned operation is lawful in the forensic context at the NFC. Despite there being no legal obstacles, FR cannot be used until a specific solution to the IT-system has been implemented.

In addition, the method developed by NFC to search images against the mugshot database has been validated and assessed by the Swedish accreditation authority (Swedac), and a positive decision for accreditation within ISO/IEC 17025 was granted to NFC in May 2020. This is possibly the first such accredited method in the world.

Also, during 2019/2020, FR technology has been used in a pilot study with video analytic software. The main purpose of the software is to cluster different sequences together showing a certain person or object. This pilot was also preceded by a legal analysis, and a consultation with the DPA and was completed in July 2020, supporting the permanent use of such a video analytic tool by the Swedish Police. The video analysis software is not planned to be connected to any database of known identities, but rather the main purpose is to help the investigators to analyse large quantities of image and video material in a more effective manner.

In addition to the implementation of FR technology for criminal investigations, the border police in Sweden are also preparing for a pilot study to compare images in passports from third-country nationals with images taken of passengers at the airport within the Entry Exit System (EES) framework. While the legal analysis gave a green light, this pilot was temporarily halted due to the DPA finding a lack of a legal framework for collecting the necessary training and testing data from passengers. The necessary laws will be in place from 1 December 2020, and the pilot will start a few days after this.

In 2021, the police fingerprint and mugshot databases will be merged into an ABIS system, with search capacities for both modalities.

1.2. Organisations involved

Within the Swedish Police Authority:

- National Forensic Centre (NFC) (data owner of the mugshot database, biometrics process owner, executer of searches);
- IT-department (FR software licence owner, implementer of IT-solution, maintainer of IT-system for mugshot database);
- Legal department (executer of legal analyses and DPA consulting).

1.3. Mugshot database

The mugshot database *(Signalementsregistret)* is technically maintained by the IT-department, with NFC as the information owner. NFC is responsible for the data, and for the processes involved in the acquisition of the data. The data is collected by police officers via booking stations where both fingerprints, images of the person and written descriptions are collected. The data is then enrolled by NFC. It is expected that in 2021 there will be a suitable IT-implementation in place for NFC to perform FR searches within the new ABIS system.

The mugshot database contains images and metadata of people that are under investigation (register of suspects) and those that have been convicted of a crime (register of convicts). Metadata stored generally include for example:

- Name and Personal/National ID number (alternatively another number for aliens, or mugshot/case ID if unknown identity). Date of birth and nationality.
- Physical/personal written attributes such as gender, height, teeth status, head shape, skin tone, hair form/colour, eye colour, nose shape, mark, scars, tattoos etc.
- A numeric value stating the crime(s) suspected or committed.
- Location/region of capture, date of mugshot capture and person performing the capture.

Along with the metadata, multiple images of every individual are stored. Generally:

- Face frontal, left and right (3 images);
- Full body images frontal, left, right (3 images);
- If relevant, images of distinguishing attributes such as scars, marks and tattoos.

As of January 2020, the number of entries in the mugshot database was around 60 000, however, the number of individuals is currently not known. There is no limit regarding how many images can be stored for one individual. The photograph and fingerprint capture session is usually conducted by police officers or arrest personnel at those police stations where the booking station equipment is available (78 stations, but will soon be increased to 100). The booking station has a specific digital camera for the images. In case of system failure, there is a manual back-up procedure. As the next step in the process, the fingerprint quality is verified by NFC fingerprint experts (currently not the mugshot image quality), before the data is enrolled into the separate databases (mugshot database for images and AFIS for fingerprints) together with metadata. If aliases are found from the fingerprints, these entries are connected in the AFIS system. Usually, a comment is also made about the aliases in the mugshot database entries, but there is no automatic connection between these entries in the mugshot database system.

Entries are automatically deleted from the mugshot database according to the legislation. The automatic deletion is determined by modifications to data in two other registers, the register of suspects and the register of convicts. In the register of suspects, an individual remains as long as there is an active criminal investigation where he/she is a suspect. In the register of convicts, an individual will be entered if he/she is convicted of a crime. In this register the individual can remain for many years depending on the nature of the crime, as long as 10 years after the sentence was fulfilled. Once all entries from an individual are removed from both the suspect and the convict registers, all entries of the individual must also be removed from the mugshot database.

Currently, uncontrolled images are not stored in any database. These images are only archived in the relevant investigative case records. Nevertheless, the aim of NFC is to create a database of such uncontrolled images for unsolved crimes (similar to the latent fingerprint database) but, before that is initiated, a legal analysis will need to take place and additional/updated legislation may need to be introduced.

In 2021, the fingerprint and mugshot databases will be merged into an ABIS system, with search capacities for both modalities. The new system will also include a new booking system and enrolment capability. With the new ABIS, all biometric data will be connected to a single identity, which will deter the inclusion of multiple identities in the databases.

1.4. Facial recognition searches

Any information regarding the FR engine is classified.

1) Testing of FR software

Prior to the pilot, several top performing algorithms in the NIST vendor tests together with other algorithms of interest were tested in-house. It was important to use a large amount of case relevant test data to properly understand the performance of the different algorithms under relevant conditions. Also, a significant amount of in-house data was used for testing as it is likely that many of the algorithms have previously been trained on publicly available data which might influence the test results. The software that was finally decided upon, was the top performer in most of the in-house testing, and was especially competent on low quality surveillance camera data.

For the purpose of further testing, validation and research, the selected FR software was then implemented and used with a clone of the Swedish mugshot database. After the initial legal analysis, this implementation was temporarily used during the pilot study.

The tests showed that, with the selected algorithm and the size of the database, if the correct person is enrolled in the database, he/she is expected to turn up on the top 20 list of best matches even with most low-quality images. For very low-quality images, it is possible that the correct person, even if present in the database, might fall outside the top 20, but in these cases the probe image quality is usually too low for a meaningful manual verification. Hence a search list size of 20 candidates was decided as a starting point for real case searches, but the number can be altered by the operator when needed.

2) Implementation plans for FR software

Once implemented, searches in the ABIS will only be permitted with special restrictions. Only forensic experts at NFC, and a few IT-administrators, will have access to the FR system. Access is granted on very strict rules, and via a secure access point. All searches are logged within a centralized logging system. The template/feature vector of the uncontrolled image will only be archived in the ABIS system until the case is finalised at NFC.

The FR system contains several different components, including algorithms for face finding, for normalizing the face image (token image), for generating templates (the searchable, digital representation of the face), and for face matching. For each frontal facial image in the mugshot database, a template is stored in the FR system template database. As entries in the mugshot database are added or deleted, the entries in the FR system will also be, via an automated real-time synchronisation to the mugshot database.

3) Method for FR searches

At the present time, all examiners for FR searches are also forensic experts in 1:1 facial image comparison, for which NFC has ISO/IEC 17025 accreditation since October 2011. The 1:1 facial image comparison is performed using the morphological method with ACE-V as described in the ENFSI DIWG best practice manual, and every year the method is evaluated by participating in the DIWG proficiency tests. The manual facial image comparison results are evaluated using the likelihood ratio framework following the ENFSI recommendation on forensic reporting. In addition, a method is currently under development where the output score from a FR system is converted to a likelihood ratio. The aim of this project is to merge the results from the manual expert comparison with that of the algorithm to maximize the total performance.

According to the laws in Sweden, automated FR searches against the mugshot database are only permitted by NFC (not the rest of the police organisation). The SOP to perform those FR searches is summarized below. The method has been validated, and was granted ISO/IEC 17025 accreditation as of May 2020.

The FR search method is in short described as follows: a request is sent by the investigator to NFC together with one or more images of the unknown person caught on imagery. It is the task of the investigators themselves to extract the best possible images from the imagery available, and NFC has provided a short guideline on how to do this. No quality limitations have yet been set, other than the limitation of the face finding algorithm. The uncontrolled image is enrolled and searched by the forensic expert, and the FR software displays a list of, usually, the 20 best matches. When deemed relevant, the list size can be adapted to any number. The search list candidates are analysed manually by the expert, using a combination of a holistic approach (usually to exclude candidates) and a morphological based analysis. The same procedure is repeated independently by a second expert (blind verification), and the results from the system output and both manual analyses are then combined to produce a final result. The result can be either a potential candidate or no candidate, and the report is in the form of an investigative lead. If no candidate is found, the investigator can, in some cases, request an extended search, where a list of the best matches is reported (but where all persons that are clearly dissimilar to the person on the probe image have been removed from the list manually by the experts).

1.5. Quality assurance

The capture of fingerprints and mugshots is done by police officers at a booking station. There is a written SOP regarding this procedure, and the police officers receive training to achieve a licence for the task. In the near future, it is planned to implement the training using the in-house e-learning platform. Training is also provided for the enrolment procedure, together with written training materials.

The frontal face images are of resolution 300 x 400 pixels in JPEG format and are taken with a digital camera which is part of the booking system. The images are captured according to homogeneously set specifications regarding the background, camera settings, camera distance etc.

The images are currently not captured according to any biometric standard, but this might change soon as there are plans to replace the current booking stations. The most interesting would be to harmonize with a standard used for central European systems (e.g. ISO/IEC 19794-5:2011 - corrected version 2016, Information technology – Biometric data interchange formats – Part 5: Face Image).

1.6. Legal framework regulating the use of facial images in relation to criminal activity

The legislative acts that regulate the use of biometric data, including the use of facial images by the law enforcement agencies, are summarized here.

EU Directive 2016/680 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.
Crime Data Law (2018:1177): This law implements the EU Directive 2016/680.

Criminal Data Act (2018:1396): This law is an addition to Crime data law (2018:1177), active when competent authorities do process personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The following is a short summary of the legal acts that were relevant in the legal analysis which was conducted before the use of FR searches against the mugshot database was implemented.

The general prohibition to search for persons based on sensitive personal data including biometric data is found in

- 2 chapter 14 § Crime Data Law (2018:1177)

The general legal basis for using personal data by competent authorities if necessary is found in

- 2 chapter 1 § Crime Data Law (2018:1177)

Personal data can be used at the National Forensic Centre if it is needed for forensic analysis, casework or comparisons

- 6 chapter 1 § first section point 2 Criminal Data Act (2018:1396)

More specifically, the National Forensic Centre can use biometric data in casework for forensic purposes according to

- 6 chapter 4 § Criminal Data Act (2018:1396)

An exception to the general search prohibition (2 chapter 14 § Crime Data Law (2018:1177)) exists for forensic casework, which makes it possible only for the National Forensic Centre to search using biometric data in the mugshot database as described in

- 6 chapter 5 § Criminal Data Act (2018:1396)

The following is a summary of the other uses of facial image data by a competent authority.

If it is of national interest, the police are allowed to share personal data with Interpol, Europol or a competent authority of another country which is connected to Interpol (7 § Criminal Data Act (2018:1396)).

The police are allowed to use an image of a person of interest from other databases, including civil databases (8 § Criminal Data Act (2018:1396)). It is not allowed to perform a FR search in civil databases for the purpose of criminal investigations.

2. Other databases and registers related to criminal activity that are not used for facial recognition

The following registers/databases are related to/part of criminal proceedings but are not allowed to be used with FR.

2.1. Database of Listed/wanted known persons

Individuals that are listed for notice are registered in a national database. However, this database does not contain any biometric data. If a person is to be listed for notice internationally, the biometric information is collected from AFIS and then submitted to SIS-AFIS.

2.2. Internal webpage of Persons of interests

Unidentified offenders captured on imagery are posted on an internal police site for a limited time period. If any police officer recognizes a person, intelligence can be provided to the investigator who posted the notice. This is a fully manual procedure.

2.3. Prison image database

The prison image database is owned by Swedish Prison and Probation Service (SPPS). As of January 2020, the database includes around 45 000 offenders consisting of around 187 000 images with several photographs retained for each individual. There is no limit regarding how many photographs can be stored for every individual. Offenders are usually photographed with a minimum of two photographs per session (one frontal and one from the right side of the face). More photographs are taken if this is required, for example, if the offender has a scar or tattoo. New photographs are taken every year and if needed when an offender changes appearance (for example, due to shorter hair or facial hair etc.). Moreover, photographs are complemented with some metadata containing known personal data about the offender. Metadata includes some physical attributes such as height, weight, eye colour, hair colour, body construction etc. The photographs are taken by specially trained prison staff and are saved in JPEG format. Photographs are taken by a standalone camera, which can be a smartphone camera or similar, and are then manually transferred to a system called the Offender Management System (OMS).

3. Civil databases

In addition to above listed databases associated with criminal activity, there are also a number of civil databases. In contrast to the criminal databases, the civil databases hold data of individuals regardless of whether they have been under suspicion or convicted of criminal activity. In other words, any Swedish civil person, without reservation for Swedish citizens, can appear in the following databases.

The passport database contains facial images that are managed through a case management system named RES. The system and the stored images are governed by the Swedish Police. Explicitly by law, these images cannot be made searchable and, thereby, current legislation prohibits the use of FR algorithms on this database.

National ID cards are also issued and managed by the Swedish Police via RES. There are also other types of ID cards that can be issued by, for example, the Swedish Tax Authority and some Swedish banks. It is not permitted to search any of the mentioned ID documentation databases with FR algorithms for criminal investigative purposes.

Swedish driver's licences are issued by the Swedish Transport Agency. The licences, which always include a facial image, are stored within a database called Road Traffic Registry. There are approximately 6.6 million driver's licence owners in Sweden, but the exact number of images stored in the database is not available. However, in addition to the driver's licence images, the Swedish Transport Agency also stores images for other record types, such as images associated with taxi driver identification and tachograph documents.

The Central Aliens Database (CUD) is the central database within the Swedish Migration Agency and contains all biographic, biometric and case related information regarding all kinds of migration matters such as asylum, visas, work permits and foreigners passports. A set of applications for handling the different case types is attached to the CUD. The number of individuals registered in the Central Alien Database is around 3 million as of January 2020. Facial images and fingerprints are stored in a separate register within the CUD and may be used for searches. Facial images and fingerprints are stored for 10 years or until a Swedish citizenship is awarded according to the Aliens Data Ordinance. There is no limit to how many images can be stored for an individual. The images primarily consist of frontal face images that are photographed by trained staff using one of the Migration Office's biometric kiosks. The biometric kiosks capture fingerprints, signatures and facial images, and have built in lighting for consistent quality. The images are captured using the ICAO standard as the guideline. The CUD also holds full biographic data, such as names, date of birth, nationality, family relations, contact details, aliases, and other information of interest with regards to migration matters. Fingerprint data is included for asylum seekers only. Currently, it is not permitted to use FR searches for criminal investigation purposes on this database. The Central Alien Database is under the regulation of the Aliens Act, the Aliens Data Act, the Aliens Ordinance and the Aliens Data Ordinance.

United Kingdom

1. Data/information collection

FR methodology is widely used within the UK in several different ways, with the technology and processes having been developed over the last decade. Thereby, the UK has wide and deep experience in the use of FR that can be shared with other countries across Europe. Nevertheless, over the course of the TELEFI project, the collection of UK data/information from public organisations has been hindered, first through the result of the UK BREXIT Referendum and, secondly, through the negative publicity arising from the significant media and public hostility to the recent police use of FR technology. These factors have led to a cautious attitude being shown towards engagement from the relevant UK organisations that has arisen from the associated political sensitivities. In particular, the UK left the EU on 31 January 2020 and the future working relationship between the UK and the EU is yet to be resolved. Thus, in the context of the TELEFI objectives, looking ahead towards a future involving the sharing of facial images between different EU countries, it is apparent that the potential involvement of the UK within such an arrangement is not at all clear. Thus, the purpose of the UK data collection within the TELEFI project has focused on documenting the current national experience to provide support for the wider TELEFI objectives.

Two TELEFI surveys were completed by representatives from:

- The Defence Science and Technology Laboratory, Dstl (an individual with extensive experience over the last decade inside several Government Departments during the growth of FR systems within the UK and the development of the associated facial image standards) and;
- The UK Home Office (an individual with experience in managing the police FR databases).

In addition, open public sources (see References) have been used (particularly the websites of various UK Government/law enforcement organisations) by consultation with numerous documents on many aspects of FR.

2. Summary of collected data

2.1. Use of facial recognition by UK law enforcement – retrospective for intelligence purposes

In the UK, images of persons caught on CCTV (say), suspected of committing a crime, can be checked against a national face image database (contained within the Police National Database, PND). The facial images on the PND are those taken by police forces of individuals detained at police stations following their arrest (under the legal mandate of Section 64A of the Police and Police and Criminal Evidence Act, PACE 1984). Thus, the facial images loaded into the PND are mainly for individuals that have already had an encounter with the police. There are 43 different Police Forces across the UK and the facial images, when first taken, are stored within local custody IT systems, and are then uploaded in batches to the PND. Starting the process in 2011, the facial images from most UK police forces are now uploaded to PND although there remain some police forces that have yet to upload all their images. There are many different local IT custody systems that are used by UK police forces and hence there are many 'local collections' of facial images in different formats (and with different search capabilities or no search capability) as well as the central PND collection.

It is estimated that the PND currently contains between 14 and 16 million custody images that have been enrolled into the FR gallery. The PND facial searching facility allows an authorised user (usually a police officer) to search through saved custody images to find potential matches against an image that has been temporarily uploaded (a 'probe' image). Police officers will generally search ‘local collections’ first and then move on the national PND search, as necessary. Facial images enrolled in PND are limited to a specified size range (10 kB to 5000 kB). Results from PND searches are returned as a list of potential matches, ranked in order of closeness of fit, facilitating a manual inspection to confirm or reject a match. Thus, matches are used for intelligence purposes and it is a tool to make manual searching more efficient.

Facial images on the PND can be searched by some other organisations, as well as the police: National Crime Agency (NCA), Ministry of Defence (MOD) and Home Office Immigration Enforcement.

The PND database was developed in conjunction with a commercial company (CGI Group Inc.) with input from the Home Office and has continued to be managed in this way. The PND became operational in 2010–2011 with police forces starting to load information. A facial search functionality went live on 28 March 2014 with software from Cognitec. It is planned that the PND will be incorporated within a new, more integrated law enforcement database for the UK in the next few years. This new system will have extensive links to other functions across the Home Office. [see Section on UK Biometric Strategy, below]

2.2. Use of facial recognition by UK law enforcement – retrospective for evidential purposes

Forensic laboratories within the UK are routinely involved in the comparison of photographic facial images for evidential purposes, with the results being used in the courts. Clearly, the requirement for such expert evidence on such matters is often the follow-on stage after an initial intelligence based automatic FR scan points towards a particular individual and, with a subsequent follow-up police investigation, this leads to a criminal charge. Several different guidance documents are used for this work:

- “Facial Identification Guidance 2009”, UK National Policing Improvement Agency.
- “Forensic Image Comparison and Interpretation Evidence: Guidance for Prosecutors and Investigators”, Issue 2, UK Forensic Science Regulator (February 2016).
- “Best Practice Manual for Facial Image Comparison”, ENFSI-BPM-D1-01 (January 2018).
- “Image Enhancement and Image Comparison: Provision of Opinion”, Regulatory Notice 01/2019, UK Forensic Science Regulator.

2.3. Use of facial recognition by UK law enforcement – live facial recognition for intelligence purposes

Several police forces in the UK have conducted operational live facial recognition (LFR) trials in recent years and, in general, all forces have used the same approach. Before commencing, they compile a ‘watchlist’ of subjects of interest and, generally, use facial images taken in custody to populate that list. They then decide when, where and how long to deploy the LFR. Deployments have included crowds at shopping centres, in the street during festivals and near sports grounds. The police use a van as a control centre, with a Commanding Officer on board and other officers on the ground amongst the crowd. The monitors in the van display the video stream from the cameras situated on the van or nearby. As people pass, the technology finds the facial images, converts them to a biometric template and compares the faces against those in the watchlist. If a potential match is found, the police officers in the van communicate with the officers in the crowd such that decisions can be made to intervene, approach, or ultimately apprehend the individual.

The Metropolitan Police Service (MPS) in London and South Wales Police (SWP) have done most of such trials (MPS - Aug 2016 to Feb 2019) / SWP - May 2017 to March 2018). Leicestershire Police and Greater Manchester Police (GMP) have also run small scale trials. The official reports describing the key trials have been published:

- "An Evaluation of South Wales Police's Use of Automated Facial Recognition" (September 2018);
- "Metropolitan Police Service Live Facial Recognition Trials" (February 2020).

From the beginning of the trials, LFR has had many critics in the UK [see the Section below]. Within London, this led to a detailed report on LFR from the London Policing Ethics Panel (LPEP), a group set up as an independent panel by the Mayor of London to provide ethical advice on policing issues that may impact on the public confidence in the capital. That report ("LPEP Final Report on Live Facial Recognition", May 2019) proposed that LFR should only be deployed operationally if a given set of specific conditions were met to ensure lawful and ethical deployments. This was followed by a letter from MPS to the Mayor of London (23 January 2020) that set out their planned detailed responses to those conditions explaining the new safeguards that had been put into place regarding the use of this technology. One area was a description of the measures that would be taken to build public confidence, including a commitment to publish the full evaluation report from the MPS trials (as described above) and other items of relevance (legal mandate, guidance document, SOP etc.). All these items are now freely available on the MPS website. A formal public announcement was made on 24 January 2020 that the MPS would start to use LFR in a routine operational manner.

Currently, MPS is the only police force in the UK to be deploying LFR routinely in everyday policing. Operational deployment started in February 2020 but has been hindered over recent months by the COVID-19 outbreak in the UK. Looking at the difficulties ahead, there are current concerns that many people will be wearing face coverings over the coming months (masks, scarfs).

2.4. Facial recognition oversight and governance

There are several independent public bodies set up by the UK Government to provide the necessary checks and balances across a broad range of law enforcement (and other) activities with reference to facial images. This work involves compliance with current relevant legislation, the identification of new legislative needs, the development of 'codes of practice' and the oversight of ethical principles. Clearly, the rapid expansion of FR work within law enforcement over recent years has raised many important matters in these areas. The independent national public bodies of interest to FR in the UK are:

- The Forensic Science Regulator (FSR)

  Monitors and maintains standards in forensic science services across the UK criminal justice system.

- The Biometrics Commissioner (BC)

  Over many years, the main task of the BC has been to review the retention and use of DNA & fingerprints by the police. However, the BC is now taking a major interest in facial images as a new biometric. BC publishes an annual report that contains much information and comment about the current handling of facial images. In addition, BC has commented publicly on specific facial image related matters that have arisen as a response to the government's Biometric Strategy in 2018. Further, a statement followed the MPS publication of their impact assessment in relation to their deployment of operational LFR (February 2020).

- The Information Commissioner's Office (ICO)

  The ICO is the UK's independent body set up to uphold information rights in the public interest, including matters relating to the police. ICO covers several areas of legislation of relevance to the handling and use of facial images including the Data Protection Act 2018 and the GDPR. ICO has also taken a special interest in LFR over recent years, has declared it as an area of high priority for ICO attention and conducted a detailed investigation into that area. A full report of this investigation was published: "ICO investigation into how the police use facial recognition technology in public places" (October 2019). At the same time, ICO published a second document "Information Commissioner's Opinion - The use of live facial recognition technology by law enforcement in public places", which provided a detailed work plan towards the future deployment of LFR.

  A public statement from ICO on 24 January 2020 acknowledged the work that had been done by the MPS (incorporating the advice from the 'ICO Opinion') in preparation for the MPS to routinely use operational LFR, as publicly announced by the MPS on the same day. The same ICO statement went on to reiterate the call to the UK Government to introduce a statutory and binding code of practice for LFR as a matter of priority.

  Further to the ICO investigation into the police use of LFR, the ICO is currently engaged in a further investigation into the use of LFR by private sector organisations, including situations where this use has involved collaboration with the police or other law enforcement bodies. The collaboration has generally involved the police supplying the facial images of individuals 'of interest' to site owners for use with their own camera installations for LFR. There have been high-profile deployments in shopping centres and railway stations. Deployments by the owners at King's Cross railway station in London came to the attention of the media in September/October 2019 with the MPS admitting that it had transferred a small number of custody images to the owner.

- The Surveillance Camera Commissioner (SCC)

  SCC promotes the development and compliance with the "Surveillance Camera Code of Practice" (June 2013) providing the guiding principles that apply to all surveillance camera systems in public places, ensuring proportionality and transparency. One of the underlying principles is to give the public confidence that surveillance cameras are deployed to protect and support them, rather than spy on them. There is a strategy document: "A National Surveillance Camera Strategy for England and Wales" (March 2017). In the specific context of FR, the SCC has a Memorandum of Understanding (MoU) in place with the ICO. In addition to the SCC annual reports, there are specific publications related to FR technology: "The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems – Section 33 Protection of Freedoms Act 2012" (SCC, March 2019) and "Data Protection Impact Assessments Guidance for Carrying out a Data Protection Impact Assessment on Surveillance Camera Systems" (SCC & ICO jointly, October 2018).

Moreover, there are specific independent groups/committees with a particular interest and focus on FR technology in the UK police service:

- Biometrics and Forensics Ethics Group - Facial Recognition Working Group (BFEG)

  The BFEG provides independent ethical advice to Home Office ministers on issues related to the use of biometrics and forensics. It operates under a published code of practice and produces a detailed annual report. A major topic on their agenda is the police use of FR systems and BFEG has produced an interim report "Ethical Issues

Arising from the Police Use of Live Facial Recognition Technology" - Interim Report of the BFEG - February 2019. The work continues and an information gathering event was planned for April 2020, but this has needed to be postponed because of the COVID-19 outbreak in the UK.

- Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board (LEFI Board)

  The Board's remit is the police forces in England and Wales and was set up with terms of reference (July 2018) to consider matters of legislation, codes of practice, best practice, quality & ethical standards, and public transparency. Meetings are held regularly with the minutes being publicly available on the government website.

- London Policing Ethics Panel (LPEP)

  A group set up as an independent panel by the Mayor of London to provide ethical advice on policing issues that may impact on the public confidence in the capital. [See Section on LFR, above]

There are other groupings within the UK Parliament that have taken a significant interest in FR matters over recent years, adding various publications to the overall discussions and debates. This interest has arisen as the public reservations about FR technology have continued to grow. Of significance are:

- Full House of Commons (the chamber containing the democratically elected Members of UK Parliament, MPs). A full debate on "Facial Recognition and the Biometrics Strategy" took place on 1 May 2019. The full transcript is available within Hansard (https://hansard.parliament.uk/Commons/2019-05-01/debates/16A45B3A-6F02-4542-B5F5-2146CA0C6AB8/FacialRecognitionAndTheBiometricsStrategy).
- House of Commons Science and Technology Committee (a cross-party group of MPs that conducts specific investigations across science & technology topics). Several investigations have dealt with FR and the biometric strategy within the UK leading to the publication of substantial reports. Two recent examples are: "Biometrics strategy and forensic services – Fifth Report of Session 2017-19" - 25 May 2018" and "The work of the Biometrics Commissioner and the Forensic Science Regulator – Nineteenth Report of Session" – 18 July 2019.

These various organisations play a very important role in the oversight and governance of FR for law enforcement within the UK. Furthermore, their engagement has sometimes been extremely critical of the approaches that have been taken, as the new FR methods in the UK have been introduced. [see the Section on Challenges and Public Opinion, below.]

2.5. Use of facial recognition in UK law enforcement – challenges and public opinion

The use of facial images in UK law enforcement has met with many strong challenges from the very beginning. Some of this has come from the media and the general public but, in parallel, many concerns have been expressed by the various groups and organisations set up by the UK Government to oversee and govern the facial image work (listed in Section 2.4 above). In turn, democratically elected politicians within the UK have listened to these critics and started to share those anxieties. This has led to the full debate in the House of Commons (May 2019). In particular, the LFR police trials have triggered the greatest worries. Facial image issues have been raised across many different organisations (ICO, BC, SCC, BFEG, LEFI Board and the House of Commons Science and Technology Committee) with areas of unease including:

- The lack of a clear retention policy for facial images maintained on local police force custody systems and on the PND. Of major concern is the legality of retaining the images of innocent individuals on databases and the fact that, currently, there are no straightforward mechanisms/processes for automatically flagging and removing those images. The wider issue is the danger that these inappropriate images might eventually appear in LFR watchlists.

- The lack of recognition that police forces must apply well-defined data protection rules in line with the Data Protection Act 2018, when deploying LFR. Notably, there is the strict necessity to apply a threshold in providing a balance between operational requirements and privacy/intrusion. At the two extremes, one might consider the targeting of a specific terrorist subject as compared to the blanket, opportunistic and indiscriminate processing of data from thousands of individuals to help identify a few minor suspects. This encompasses the general principle on how the individuals are selected to appear on the watchlists.
- Concerns that the images imported into an LFR watchlist may not be legally obtained and/or are not of adequate quality.
- The lack of a statutory and binding code of practice for LFR work by police forces.
- A lack of transparency in educating the public about all aspects of LFR, including the technological principles and their legal rights. This has led to a lack in public trust even though people generally recognise the public safety benefits of the technology. LFR represents a significant leap away from the conventional use of CCTV and, thereby, needs much background work to raise public confidence.
- A lack of sufficient training for those within the policing community who use LFR to ensure that they are fully aware of the technical and legal limitations. There have been controversial incidents, for example, an individual was fined after covering their face when seeing an LFR deployment was underway in the street.
- Concerns related to the number of ‘false matches’ in LFR and technological biases in the underlying algorithms, particularly those associated with ethnicity.
- The use of LFR within private organisations, particularly in situations where this use involves collaboration with a police or other law enforcement body, e.g. supplying facial images for watchlists. [ICO are currently conducting a specific investigation in this area.]
- Lack of key policy documents for LFR deployment by police forces.

Adding to these areas of concern from government bodies, there have also been some reservations from academia. An independent report on the MPS LFR trials was produced by the University of Essex: “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology” (July 2019). The report was based on researchers observing some LFR deployments, beginning in June 2018, with the work centred on the overall governance of the LFR trials, the procedures and practices in operational settings and the human rights compliance. The authors had many concerns about the LFR work as it was conducted at the time.

A further significant challenge to the LFR work arose from a court case brought against South Wales Police (SWP). The case - R (Bridges) v Chief Constable of SWP, involved a member of the public having concerns that the SWP LFR trial deployment may have captured his image from a police van while he was out shopping in Cardiff city centre. He brought the case, to ask the High Court to decide whether the use of FR in this way was lawful. The case was heard in May 2019 with the judgement on 4 September 2019 which held that it was lawful for the police to use automated FR software. The High Court decided that while FR does interfere with the privacy rights of everyone scanned, the current legal framework does provide sufficient safeguards. Application was made to appeal against this judgement and in November 2019 the Court of Appeal granted permission to proceed on all grounds. The hearing took place in the summer of 2020 and the Judgement was published on 11 August 2020. The UK Court of Appeal unanimously reached a decision against the face recognition system used by SWP calling the use of automated face recognition “unlawful”. The Court said that three out of the five arguments put forward by Bridges in their case were valid, including the lack of guidance and rules as to when a police force could use LFR and who would be included on the watchlist database. The Court also said that the police force had not tried to understand whether the system being used was biased depending on a person's gender or race. The Court held that the existing legal regime for LFR was not robust enough to enable police to use the technology lawfully. Following the judgement, there have been different interpretations and disagreements about the exact consequences for the future use of LFR in the UK.

A further strand of the challenges to the use of FR technology in UK policing has arisen from the regular campaigning work of two human rights organisations, looking to reduce the use of FR technology. Liberty (www.libertyhumanrights.org.uk) is the main supporter of the R Bridges v Chief Constable of SWP case. Big Brother Watch (https://bigbrotherwatch.org.uk) is also running a very vigorous campaign against FR and, along with many other activities, has produced a substantial report: "Face Off – The Lawless Growth of Facial Recognition in UK Policing" (May 2018).

2.6. Facial recognition in the UK biometric strategy

The Home Office published its Biometrics Strategy in June 2018. In addition to the traditional fingerprint and DNA areas, facial images were given a prominent position in the way ahead, being one of the "new biometrics" emerging from recent technological developments. The increased digitisation of facial images, combined with software to facilitate reliable image matching, has changed the use of the facial biometric across the Home Office sector. The document addressed the current and future uses of biometrics within the Home Office (the identification of crime suspects and the verification of people in immigration and nationality systems), but does not address the use of biometrics by other UK Government Departments. The strategy re-emphasised the Home Office plans to integrate its various biometric services, which are currently based on various separate legacy platforms, limiting their functionality, and restricting the sharing of data between the different functions. It also actively promotes the idea of sharing and matching facial images in the Home Office sector with other Government Departments. Emphasis was placed on the need for these sharing activities to be developed and implemented in ways that ensure full compliance with the complex legal framework within the UK.

One of the specific Home Office actions within the Biometrics Strategy was the establishment of the LEFI Board to provide policy recommendations regarding the use of facial biometrics and the future oversight arrangements.

The Biometrics Strategy confirmed that the current Home Office plans to integrate biometric services (including facial images) will be implemented through the Home Office Biometrics (HOB) programme which is focused on 3 biometric modalities (fingerprints, DNA and facial images). HOB will deliver cross-department services for the identification and verification of individuals to many different organisations including police forces, the National Crime Agency (NCA), HM Passport Office (HMPO), Border Force, UK Visas & Immigration (UKVI) and other Government Departments (e.g. the Ministry of Defence). It is proposed that while all the biometric collections will be physically within the same system, they will be logically separated with 'role-based access controls' allowing individuals to access the data and activities they are permitted to use. With reference to facial images, existing legacy databases have been included within the HOB scope: image database within the Immigration and Asylum Biometrics System (IABS) and the images within the Police National Database (PND).

Another Home Office work programme, the National Law Enforcement Data Programme (NLEDP) is underway and is a relatively small part of the larger HOB programme. NLEDP will combine the currently separate PND (that includes the national police collection of facial images as uploaded from local custody collections) and the Police National Computer (PNC) system. PNC, first introduced in 1974, holds personal data and other information about individuals together with information about vehicles and property. PNC is a text-based depositary of local police force information and is separate from the local custody record databases that hold the original facial images that were captured by the police. Recent comment from the Home Office (March 2020) suggests that the NLEDP is running behind schedule but a phased approach starting in 2020 is on track for completion in 2023.

The publication of the Biometrics Strategy in 2018 stimulated much commentary and debate around that time, some critical. The Biometrics Strategy and the Home Office Programmes (HOB and NLEDP) were all part of the debates. The Biometrics Commissioner (BC) and the Biometrics and Forensics Ethics Group (BFEG) made specific inputs. In parliament, a full debate took place in the House of Commons ("Facial Recognition and the Biometrics Strategy", May 2019) and a report was produced by the House of Commons Science and Technology Committee ("Biometrics Strategy and Forensic Services", May 2018).

2.7. Collection and retention of custody images

A facial image capture standard has been in place within the UK since 2007, "Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark & Tattoo Images". It is a detailed technical document that specifies the requirements for the capture of facial/mugshot images whilst also defining the image compression and interchange format requirements for the exchange of the captured images and associated image data. This is often referred to as the "FIND Standard" (**F**acial **I**mages **N**ational **D**atabase). The standard was used as the basis for the creation of the PND image collection from 2010 onwards.

The legality of the continued police retention of custody images for unconvicted individuals has been challenged in the High Court (2012). It was held that it was unlawful without case by case consideration. The Home Office responded to the judgement, with the publication of a "Review of the Use and Retention of Custody Images" (February 2017) that did not introduce automatic 'weeding' but provided the right for an arrestee to make a request to the Chief Officer to have their facial image deleted. This remains a controversial area as it appears that the automatic 'weeding' of images is not technically possible and that will remain the situation until the new software platform (LEDS) is implemented. In the meantime, the process of responding to requests sent to Chief Officers has been handed to the College of Policing for implementation. The College's recommended process for responding to requests for the facial image deletion is available on their website: "Information Management – Retention, Review and Disposal".

2.8. Legislation

There are many pieces of UK legislation that are relevant to the capture, storage (databases, retention, disposal etc.) and the use of facial images for law enforcement purposes and for other government functions. There are various references to specific UK legislation within the relevant sections of this report, but those are not a complete list. A comprehensive overview of all UK legislation can be found at: www.legislation.gov.uk [The official home of all UK legislation]

It should be noted that the UK involves four separate counties (England, Wales, Scotland and Northern Ireland) and that there are various aspects of devolved administration between the counties and there are areas where the law diverges, although much of the legislation is common throughout the UK. The legislation differences in the different countries are also presented on the www.legislation.gov.uk website, along with EU legislation that applies to the UK at the present time and will continue to do so until the final BREXIT transition is complete.

3. UK civil databases

There are other national databases in the UK that contain significant numbers of facial images. In comparison to most countries in Europe, the UK does not issue 'Identity Cards' and thereby there is no database containing facial images associated with such a system. The main document for international travel is the passport that is often used to verify one's identity, as necessary. Nevertheless, there is no obligation for a UK citizen to own a passport and, furthermore, there is no requirement for a UK citizen to carry any type of identity documentation as one travels around the UK.

These are the main national databases containing facial images:

- Her Majesty's Passport Office (HMPO) Passports Main Index - Home Office

  As part of its normal business, HMPO collects facial images which it stores in this database. These are used as an aid to decision making during an application for a UK Passport and for the issue of the passport document. HMPO Main Index does not contain any other biometrics other than facial images. The HMPO Passports Main Index has built in search capability for facial images.

  All passports issued to UK citizens since September 2006 are 'biometric', having an electronic chip that contains the personal information, along with the digitised version of the facial image as shown on the passport pages. The chip does not contain any extra information other than that already printed on the passport. In this way, passports are extensively used to verify identity by comparing a live image of an individual, at the time the document is presented, with the digital details in the passport chip (e.g. e-gates at airports).

  The facial images stored on the HMPO Main Index are collected in line with the HMPO guidance ("Photographic Standards Policy", 2012) describing the quality and appearance required for passport photographs. This guidance meets the standard set by the ICAO.

  A recent Freedom of Information (FOI) request indicates that the number of valid passports (with 'British Citizen' status) as of 31 December 2019 was 51.1 million, which must also represent an estimate for the number of facial images within the HMPO database. Clearly, a significant proportion of the UK population owns a passport, as the estimate for the total UK population at that time was around 67 million.
  HMPO is permitted to share information held on the HMPO Main Index with other Government Departments and law enforcement where there is a statutory power in place that permits the data sharing to occur. This can involve the sharing of personal information and facial images, as appropriate. In addition, HMPO may share information (including facial images) with overseas law enforcement agencies (e.g. Interpol) for the purpose of preventing, investigating and prosecuting crime and fraud overseas.

- Immigration and Asylum Biometrics System (IABS) - Home Office

  IABS (containing both facial images and fingerprints) provides biometric enrolment, identification, identity management and verification services within the UK immigration and citizenship domains. The system went live in February 2012. The facial images that are stored in IABS can arise from, and are used by, several different organisations and functions:
  - Border Force checks live facial images against the images contained in travel documents, as produced at the point of entry/departure from the UK. The same

checking functionality occurs at e-gates [see UK Passport's, above]. Further, Border Force officers, in certain circumstances, can use immigration powers to collect a facial image from an individual and this image is loaded into IABS.

- UK Visas and Immigration (UKVI) collect facial images as part of their normal business, for example, as part of an asylum claim, a visa/entry clearance or Biometric Residence Permit application. These facial images are stored in IABS.
- Applications for British Citizenship involves the collection of facial images from individuals, with storage in the IABS. The facial images are also stored on a separate Case Immigration Database (CID), a database that only contains facial images (not fingerprints). When the individual becomes a British Citizen, the facial image is removed from IABS but is retained on CID until the individual obtains a UK Passport at a later stage.
- Immigration Enforcement collect facial images when serving removal directions and from asylum applicants. These are stored on IABS.

In 2015, IABS was reported to contain the facial images of around 15.5 million people (along with their fingerprints). No further up-to-date information has been located. IABS has built in facial search capabilities. The information in IABS can be accessed by law enforcement where there is a statutory power in place that permits the data sharing to occur.

- Driver & Vehicle Licensing Agency (DVLA) - Department of Transport

The Driver & Vehicle Licensing Agency (DVLA) is an executive agency, sponsored by the UK Department of Transport. All Driving Licences in the UK are issued by DVLA. All those issued before 31 March 2000 were paper based and did not include a photograph. Such old-style paper licences remain valid until the driver reaches the age of 70. All Driver Licences issued to new drivers (and all licence replacements) after 31 March 2000 have been plastic photocards which display a facial image of the driver. These photocards have a 10-year expiry date (or 3-year expiry date for those issued to people over 70). There has never been an obligation to upgrade from an old-style paper licence to a photocard other than when the paper licence reaches its expiry date.

Thus, there remains a mixture of old-style paper licences and photocard licences across the UK population. In December 2019, there were 49.9 million Driver Licences registered with the DVLA (including both 'full' and 'provisional' licences for learner drivers). In 2015, the DVLA indicated that there were approximately 7 million UK drivers with old-style paper licences, but it is highly likely that the number of paper licences has decreased after that date. Hence, as a conservative estimate, there are at least 43 million photocard Driving Licences registered with the DVLA. Thus, this must represent the number of facial images stored on the DVLA database.

The application process for a Driving Licence to the DVLA (new or replacement) can involve different ways for capturing the facial image of the driver. It can involve a paper hard copy photograph or a digital image with optional methods for verifying such images. It can also involve giving permission to DVLA to obtain a passport image from HMPO or to use HMPO as a means of verifying a separate image.

The photograph is processed at DVLA in such a way as to print the facial image on the photocard. The facial image that appears on the Driving Licence is held electronically in the DVLA's driving licence database. It is noteworthy that the DVLA does not use any FR technology to search the images in the database. Subsequent viewing of the images by the DVLA is confined to those staff with an operational need to see and use the images for legitimate and lawful purposes. The DVLA does share images with other organisations on a case-by-case basis in line with the appropriate legislation. Such sharing is done for the identification, apprehension, and prosecution of offenders.

4. Law enforcement variations for other UK jurisdictions

The UK involves four separate counties (England, Wales, Scotland and Northern Ireland) with various aspects of devolved administration. Thereby, not surprisingly, there are some differences of policy on facial image matters between the different countries. This, report does not provide a comprehensive oversight of all these differences. However, it does provide an example of how a topic can be handled in a different way within one of the UK countries (Scotland).

An Independent Advisory Group on the Use of Biometric Data in Scotland was established by the Scottish Government in 2017, to consider the use and retention of biometric data in Scotland and a report produced by that group in March 2018 contains an extensive review of the topic. The recommendations included the introduction of legislation in Scotland to establish a Code of Practice covering the acquisition, retention, use and disposal of all existing, emerging and future biometrics for Police Scotland, the Scottish Police Authority and other bodies in the field of law enforcement. Further, it was recommended that an independent Scottish Biometrics Commissioner should be created. The Bill in the Scottish Parliament to create the new Biometrics Commissioner was eventually passed on 10 March 2020 and, when appointed, that individual will oversee the delivery of the Code of Practice.

In parallel, Police Scotland and the Scottish Police Authority published a 10-year strategy "Policing 2026: Serving a Changing Scotland" (June 2017). That strategy included the introduction of several new approaches including the introduction of FR technology. The Justice Sub-Committee on Policing (a group of Scottish Members of Parliament, MSPs) launched an enquiry into how policing in Scotland makes use of FR technology. The remit of the enquiry was to consider whether the use of FR technology by the police service in Scotland is lawful, ethical, necessary, proportionate, and transparent. A call for evidence was made on 4 October 2019 and the final report was delivered on 11 February 2020. Based on the evidence gathered, that report delivered a negative conclusion regarding the potential use of live facial recognition (LFR) in Scotland. The Sub-Committee believes that this approach is "currently not fit to use" and there would be "no justifiable basis for Police Scotland to invest in this technology". The report goes on to say that "Prior to any decision to introduce live facial recognition technology to policing in Scotland, it is essential that a robust and transparent assessment of its necessity and accuracy is undertaken, and that the potential impacts on people and communities are understood". Police Scotland have now said they will conduct a public consultation on the LFR software and keep a watching brief on the use of the technology in England and Wales. Thus, the nations within the UK are not taking a totally parallel course in the introduction of FR technology.

Organisation reports

Europol

1. Facial recognition in Europol

1.1. Summary of current situation

Europol has two sub-units that use FR – the European Counter Terrorism Centre (ECTC) and the European Cybercrime Centre. This report describes the use of FR by ECTC.

Europol ECTC implemented automated FR in 2017. The same year, Europol ECTC's FR database became operational. The FR search tool and database are both known as FACE and run on software developed in-house.

The FACE database contains both controlled and uncontrolled facial images submitted by Europol Member States and Third Parties that have an operational agreement with Europol. These images are from various groups of persons involved in a criminal procedure (e.g. suspects, victims etc.). Images are entered into and searched at FACE by officials of Europol. Searches are performed against controlled and uncontrolled images stored at FACE. Requests for FR searches are submitted by and search results are reported to Europol Member States and Third Parties. FR search results are meant to be used for intelligence and not as evidence in court. Europol does not perform manual 1:1 facial image comparisons.

Legally, FR work at Europol is regulated by the Europol Regulation.

1.2. FACE

FACE is a dedicated database, developed in-house, for storing facial images (both, controlled and uncontrolled). It is populated with controlled images from Europol Member States and Third Parties. It is also populated with uncontrolled facial images that are extracted from propaganda and other relevant materials stored in the Europol Check-the-Web portal.

According to Art. 18 of the Europol Regulation[27], Europol can process personal data (including visual images and other information on appearance and forensic identification information) for the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations on:

(a) Persons who, pursuant to the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;

(b) Persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent;

(c) Persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings;

(d) Persons who have been the victims of one of the offences under consideration or with regard to whom certain facts give reason to believe that they could be the victims of such an offence;

(e) Contacts and associates; and

(f) Persons who can provide information on the criminal offences under consideration.

[27] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

Europol Member States and Third Parties who capture and submit facial images to Europol (taken from the front, both sides and both ¾ sides) do not have direct access to FACE. Instead, facial images are entered in the database by accredited Europol officials.

As a rule, all submitted images for a known individual (regardless of the pose) will be stored in FACE. If multiple similar images are submitted for a certain known individual within the framework of an ongoing investigation, Europol officials who are responsible for performing the FR searches, will select and process only a selection of them (typically, the most representative ones).

Besides images, FACE includes information about a contribution file and crime, but not other biometric or biographic data. FACE is currently a standalone database that is not linked to Europol's information management system.

Facial images are retained in FACE according to the time-limits for storage and erasure of personal data that are stipulated in Art. 31 of the Europol Regulation.

1.3. Facial recognition searches

A FR tool used for performing FR searches has been developed in-house. It is based on open-source components and is also known as FACE. FR searches at FACE are performed by accredited Europol officials of the European Counter Terrorism Centre.

Probe images that are searched against FACE do not have particular requirements, however, pre-processing (e.g. resizing etc.) of images before performing FR search is allowed only when the first search attempt has failed. The search is simultaneously performed against controlled and uncontrolled images, as both image types are stored in the FACE database. The search results in a list of candidates. The number of posts in the candidate list can be either 10, 50, 100 or 200, and this can be selected by the official performing the search. A score threshold is available, but is not used as a criterion to decide on the likeliness between the probe and candidates returned. No "lights out" scenario is used.

FR search results are reported to Europol Member States and Third Parties that placed the request for a search if there are no data sharing restrictions. Positive search results are reported as a "likely candidate" but the term "match" is not used. At this time, a scale of conclusion for reporting is not applied.

Europol FR search results are to be used as investigative leads to identify suspects and other relevant persons of interest. The search results are not to be used as evidence in court. It should be noted that Europol does not perform manual 1:1 facial image comparisons.

FACE statistics on the annual number of FR searches conducted, the number of hits achieved and the "match rate" cannot be released. Nevertheless, the number of incoming requests to preform FR searches has been increasing steadily.

1.4. Quality assurance

As the facial images that are entered in FACE are captured by the authorities in Europol Member States and Third Parties, Europol has no direct influence on the image quality other than raising awareness on the benefits of properly captured facial images. The only requirement regarding images is the file format. The FACE database can accept only JPEG, PNG and GIF files.

Europol officials who enter facial images in FACE and perform FR searches are accredited to carry out these tasks and must have received minimum training in facial comparison and identification. In addition, an internal written guideline has been developed, that is partially based on relevant documents from FISWIG and ENFSI.

The quality assessment of images follows the fundamentals of the ACE-V workflow as described within the ENFSI Best Practice Manual for Facial Image Comparisons (5.3.1. Analysis, p. 13). Typically, Europol officials will discard an image and will not proceed with a FR search against the FACE database when the quality of the image is not sufficient.

The processing of probe images follows the FISWG guideline ´Standard Practice/Guide for Image Processing to Improve Automated Facial Recognition Search Performance´. In case of a positive search result from using a pre-processed probe, the processing steps needs to be documented and mentioned in the FR search report and the pre-processed probe needs to be presented alongside the original probe image.

1.5. Legal framework regulating the use of facial images by Europol

Europol has the legal right to have a FR database and to perform FR searches according to the Europol Regulation.

Art. 18 of the Europol Regulation and ANNEX II to the Regulation specifies the categories of personal data that can be collected and processed, including the means of identification such as visual images and other forensic identification data.

Interpol

1. Facial recognition in Interpol

1.1. Summary of current situation

Interpol implemented automated FR in November 2016. Interpol's FR tool and FR database is known as the Interpol Face Recognition System (IFRS).

IFRS contains controlled and uncontrolled images from Interpol Member Countries where Interpol has an agreement with those countries for the use of the face modality. The number of Interpol Member Countries that permit the storage and searching of facial images is currently 179. Images in IFRS are from wanted persons, missing persons and dead bodies of unknown identity. Images are entered and searched in IFRS by Interpol officers. Queries for FR searches are submitted by and search results are reported to Interpol Member Countries. Searches are performed against all the images (controlled and uncontrolled) that are stored in IFRS. FR search results are meant to be used for intelligence purposes and not as evidence in court. Upon request, Interpol performs manual 1:1 facial image comparisons, however, facial image comparison reports are not delivered.

Legally, FR work at Interpol is regulated by the ´INTERPOL's Rules on the Processing of Data´.

1.2. IFRS

The IFRS runs on software from Idemia and stores facial images submitted by the Interpol Member Countries. The majority of these images are controlled images from wanted persons, missing persons and dead bodies of unknown identity. Uncontrolled images (e.g. from CCTV) are also submitted for storage in the database. However, such images do not often meet the quality requirements for storage and, typically, are only searched against the IFRS. Images are entered into IFRS by Interpol officers.

As of November 2020, the number of individuals registered in IFRS is approximately 80 000. Further, the number of images exceeds that number because several images per individual can be stored.

At the present time, IFRS contains only frontal face images, however, side views and images from an angle may be included in the future to help in the evaluation process of FR search results.

In addition to images, metadata are stored in IFRS such as name of the country that submitted an image/query for FR search and a unique Interpol identifying number. Biographic data that is sent together with the image is held in a separate Interpol system and is checked against the system before the image is entered into IFRS. Other biometric data (i.e. fingerprints and DNA) are held in dedicated databases and are not linked to IFRS. However, other biometric data from a person can be accessed in these dedicated databases using the same unique identifying number.

All facial images are retained in IFRS for 5 years. If this time is due, the Member Country is automatically notified that the end of the retention time has arrived. If needed, the Member Country has the possibility to extend the retention time for another 5-year period.

1.3. Facial recognition searches

Images submitted by the Interpol Member Countries are searched against all images (controlled and uncontrolled) that are stored in IFRS. No pre-processing of probe images is permitted. FR searches are performed by 4 trained Interpol officers using Morpho Face Investigate software from Idemia. The last update of the algorithm was in 2018.

The search result is a list of candidates where only one image per person (the most likely one) appears in the list based on a decision made within the algorithm. Candidates in the list are peer reviewed by at least two qualified officers. The search results are reported to the Member Country that submitted the query, either as a ´potential candidate´ or ´no candidate´. In the case of a disagreement about a search result, the result is reported as ´inconclusive´. No “lights out” scenario is used.

Interpol FR search results are to be used only as investigative leads and not as evidence in court. According to search statistics, there are around 300 hits reported annually.

1.4. Quality assurance

As facial images that are entered in IFRS are captured by the authorities in Interpol Member Countries, Interpol has produced a guideline ´INTERPOL Facial Images Best Practices Guide´ for support purposes. This document is mostly based on the relevant FISWG document. Acceptable file formats for images to be used in IFRS are JPEG, PNG, BMP and TIFF.

All the images that are stored in IFRS must be compliant with the requirement of having 40 pixels between the centres of the eyes. To ensure compliance, images undergo a manual control before being entered into the database. In addition, IFRS includes specific software (ASTEK) that is used for the quality control of images after they have been entered into the database.

Interpol officers who enter facial images in IFRS have undergone on-the-job training. Officers who perform FR searches have been trained by the FBI on facial comparison and must have at least two years of work experience in the FR field before being recruited by Interpol. In addition, a written SOP is available for both the entry of images and the performance of the searches.

Interpol officers who perform FR searches participate in ENFSI’s annual proficiency tests on 1:1 facial image comparisons.

Interpol plans to implement a new FR system that will be able to process CCTV footages in the next 2-3 years.

1.5. Legal framework regulating the use of facial images by Interpol

The legal requirements on the use of facial images by Interpol are stipulated in ´INTERPOL’s Rules on the Processing of Data´.

References

1. Organisations list for UK report

This is a list of the various organisations, groups and resources that proved to be relevant to the UK report. The links to the various internet websites are included. These gateways were the starting points when gathering information to describe the current UK situation.

- UK Government Website
  www.gov.uk
- UK Parliament Hansard [detailed records of UK parliamentary proceedings]
  https://hansard.parliament.uk
- UK legislation website (the official home with details of all UK legislation)
  www.legislation.gov.uk
- Home Office
  www.gov.uk/government/organisations/home-office
- House of Commons Science and Technology Committee
  https://committees.parliament.uk/committee/135/science-and-technology-committee-commons
- Driver & Vehicle Licensing Agency (DVLA)
  www.gov.uk/government/organisations/driver-and-vehicle-licensing-agency
- HM Passport Office (HMPO)
  www.gov.uk/government/organisations/hm-passport-office
- Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board (LEFI Board)
  www.gov.uk/government/groups/law-enforcement-facial-images-and-new-biometrics-oversight-and-advisory-board
- Biometrics and Forensics Ethics Group (BFEG)
  www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group
- Forensic Science Regulator (FSR)
  www.gov.uk/government/organisations/forensic-science-regulator
- Office of the Biometrics Commissioner (BC)
  www.gov.uk/government/organisations/biometrics-commissioner
- Information Commissioner’s Office (ICO)
  https://ico.org.uk
- Surveillance Camera Commissioner (SSC)
  www.gov.uk/government/organisations/surveillance-camera-commissioner
- The College of Policing (CoP) [the professional body for everyone who works for the police service in England and Wales]
  www.college.police.uk
- The Metropolitan Police Service (MPS)
  www.met.police.uk
- South Wales Police (SWP)
  www.south-wales.police.uk/en/home
- The Scottish Parliament
  www.parliament.scot
- Liberty
  www.libertyhumanrights.org.uk
- Big Brother Watch
  https://bigbrotherwatch.org.uk

2. Specific reference documents used for UK report

This section contains a list of the key documents that were used in the compilation of the UK report and the internet links to those documents, to provide convenient access. It is not intended to be a complete list of all the documents that were used in the preparation of the report, nevertheless, it does represent a good starting point for all the information reported.

"Biometric Technologies", Houses of Parliament (Office of Science & Technology) Postnote Number 578 (June 2018).
https://post.parliament.uk/research-briefings/post-pn-0578
"Facial Recognition and the Biometrics Strategy", House of Commons Library Debate Pack Number CDP 2019/0099 (30 April 2019).
https://commonslibrary.parliament.uk/research-briefings/cdp-2019-0099
"Home Office Biometrics Strategy" (June 2018).
www.gov.uk/government/publications/home-office-biometrics-strategy
"Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark & Tattoo Images", National Police Improvement Agency (NPIA), version 2.0 (May 2007).
www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/npia-capture-and-interchange-standard-for-facial-and-smt-images.pdf
"Ethical Issues Arising from the Police Use of Live Facial Recognition Technology", Interim report from the BFEG (February 2019).
www.gov.uk/government/publications/police-use-of-live-facial-recognition-technology-ethical-issues
"Biometrics and Forensics Ethics Group: Annual Report 2018" (5 May 2020).
www.gov.uk/government/publications/biometrics-and-forensics-ethics-group-annual-report-2018
" Annual Report of the Biometrics Commissioner for 2018 " (27 June 2019).
www.gov.uk/government/publications/biometrics-commissioner-annual-report-2018
"ICO Investigation into how the Police Use Facial Recognition Technology in Public Places" (31 October 2019).
https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
"Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places" (31 October 2019).
https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
"ICO statement in response to an announcement made by the Metropolitan Police Service on the use of live facial recognition" (24 January 2020).
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-statement-in-response-to-an-announcement-made-by-the-met-police
"Data Protection Impact Assessments: guidance for carrying out a data protection impact assessment on surveillance camera systems", SCC and ICO Joint Publication (22 October 2018).
www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras
"The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems", SCC (March 2019).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf
"Surveillance Camera Code of Practice", SCC (June 2013).
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
"Review of the Use and Retention of Custody Images", Home Office (February 2017).
www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

"Information Management – Retention, Review and Disposal", College of Policing website page. [Current UK guidance on dealing with requests to Chief Officers from persons to have their facial images deleted from police databases.]
www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#group-1-certain-public-protection-matters

"Fact Sheet on Live Facial Recognition Used by Police", Home Office (4 September 2019).
https://homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police

"An Evaluation of South Wales Police's Use of Automated Facial Recognition", Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University (September 2018).
http://afr.south-wales.police.uk/cms-assets/resources/uploads/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf

"Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", Pete Fussey & Daragh Murray, University of Essex (July 2019).
http://repository.essex.ac.uk/24946

"Metropolitan Police Service Live Facial Recognition Trials", Metropolitan Police Service and the National Physical Laboratory (February 2020). [Official report on the MPS LFR trials.]
www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf

"Final Report on Live Facial Recognition", London Policing Ethics Panel (May 2019).
www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf

"MPS Response to the London Policing Panel Final Report on Live Facial Recognition Technology", Letter from MPS to Mayor of London" (23 January 2020).
www.london.gov.uk/sites/default/files/mayor_of_london_-_lfr.pdf

"Live Facial Recognition", Metropolitan Police Service (2020) [A web page for the general public, providing detailed information about the steps that the MPS has put into place to prepare for the deployment of LFR in routine operational policing. Links are included to all key documents.]
www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition

"The Work of the Biometrics Commissioner and the Forensic Science Regulator", House of Commons Science and Technology Committee, Nineteenth Report of Session 2017-19 (18 July 2019). [Contains major sections on 'Automatic/Live Facial Recognition' and 'Retention of Custody Images'.]
https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf

"Biometrics Strategy and Forensic Services", House of Commons Science and Technology Committee, Fifth Report of Session 2017-19 (25 May 2018). [Contains major sections on 'Deletion of Facial Images from Police Databases' and 'Facial Recognition and Watchlists'.]
https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf

Hansard, Report of a Full Debate in the House of Commons on 1 May 2019 entitled "Facial Recognition and the Biometrics Strategy".
https://hansard.parliament.uk/Commons/2019-05-01/debates/16A45B3A-6F02-4542-B5F5-2146CA0C6AB8/FacialRecognitionAndTheBiometricsStrategy?highlight=biometrics%20debate#contribution-E7656644-2A6B-4CCB-BD2E-0D639A3D20E9

"Best Practice Manual for Facial Image Comparison – ENFSI-BPM-D1-01 version 01", ENFSI.
http://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf

"Facial Identification Guidance 2009", National Police Improvement Agency (NPIA).
http://library.college.police.uk/docs/acpo/facial-identification-guidance-2009.pdf

"Image Enhancement and Image Comparison: Provision of Opinion", Regulatory Notice 01/2019, Forensic Science Regulator (17 July 2019).
www.gov.uk/government/publications/image-enhancement-and-image-comparison-provision-of-opinion

“Independent Advisory Group on the Use of Biometric Data in Scotland”, Scottish Government (March 2018).
www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2018/03/report-independent-advisory-group-use-biometric-data-scotland/documents/00533063-pdf/00533063-pdf/govscot%3Adocument/00533063.pdf

“Facial Recognition: How Policing in Scotland Makes Use of this Technology”, Justice Sub-Committee on Policing, The Scottish Parliament, SP Paper 678 (11 February 2020).
https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology/JSPS0520R01.pdf

“Face Off – The Lawless Growth of Facial Recognition in UK Policing”, Big Brother Watch (May 2018).
https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

“High Court of Justice - Case Law Judgement: R (Bridges) v Chief Constable of South Wales Police” (4 September 2019).
https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

“Home Office Biometrics Programme – Privacy Impact Assessment”, Home Office version 1.5 (2 May 2018).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721096/HOB_Programme_Privacy_Impact_Assessment__Final_.pdf

“National Law Enforcement Data Programme: Law Enforcement Data Service (LEDS) – Privacy Impact assessment Report”, Home Office (July 2018).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721542/NLEDP_Privacy_Impact_Assessment_Report.pdf

“Privacy Information Notice”, Her Majesty’s Passport Office (November 2019).
www.gov.uk/government/publications/hmpo-privacy-information-notice

Appendices

Appendix 1: List of surveyed authorities

Country /organisation	Authority
Austria	Federal Ministry of Interior, Criminal Intelligence Service, Office 6.3 – Crime Scene
Belgium	Federal Police Belgium
Bulgaria	Ministry of Interior, Research Institute of Forensic Science, section “Identification Examinations”
Croatia	Forensic Science Centre “Ivan Vučetić”
Czech Republic	Institute of Criminalistics, Police of Czech Republic
Cyprus	Cyprus Police Criminalistic Services
Denmark	National Forensic Centre, Danish National Police
Finland	National Police Board
	National Bureau of Investigation
	National Police Board, Police Operations Unit
	National Bureau of Investigation, Intelligence Unit
France	The Central Directorate of the Judicial Police, National Division of Criminal Documentation and Coordination of the Technical Police
	Criminal Intelligence Service of the National Gendarmerie
	Forensic Institute of the National Gendarmerie
Germany	Federal Criminal Police Office, Development and Quality Management Face Recognition
	Federal Police Headquarters, Department 3 – Counter Crime, Section 33
	State Criminal Police Office Berlin, Forensic Science Institute
	Bavarian State Criminal Police, Office of Criminal Investigation
Greece	Hellenic Police Forensic Science Division
Hungary	Ministry of Interior, Department for Schengen Matters & User Management
Ireland	Civil Justice and Equality, Department of Justice and Equality
Italy	National Police
	Carabinieri
Latvia	Ministry of Interior, Information Centre
Lithuania	Ministry of Interior, Information Technology and Communications Department
Luxembourg	Grand Ducal Police
Malta	Malta Police Force
Netherlands	Centre for Biometrics, Dutch National Police
Poland	Document Examination and Audio-Visual Techniques Department, Central Forensic Laboratory of the Police
Portugal	Forensic Laboratory of Judiciary Police
Romania	General Inspectorate of the Romanian Police, National Forensic Institute
Slovakia	Institute of Forensic Science, Presidium of the Police Force
Slovenia	General Police Directorate, National Forensic Laboratory
Spain	National Police
	National Police - Special Systems Headquarters – R & D & I Group
UK	UK Home Office
	Defence Science and Technology Laboratory
Europol	European Counter Terrorism Centre

Appendix 2: List of interviewed authorities

Country/ organisation	Authority
Austria	Federal Ministry of Interior, Directorate V – Immigration, Unit V/1/b – Integrated Foreigner Administration and Innovations
	Federal Ministry of Interior, Criminal Intelligence Service, Office 6.3 – Crime Scene
	Federal Ministry of Interior, Section III – Law, Ref. III/3/a – Passports
Bulgaria	Ministry of Interior, Research Institute of Forensic Science, sections “Identification Examinations” and “Forensic Technics“
Croatia	Forensic Science Centre “Ivan Vučetić”
	Ministry of Interior, Directorate for Immigration, Citizenship and Administrative Affairs
Czech Republic	Institute of Criminalistics, Police of Czech Republic
Cyprus	Cyprus Police Criminalistic Services
Denmark	National Forensic Centre, Danish National Police
	Danish National ID-Centre, Ministry of Immigration and Integration
Estonia	Estonian Forensic Science Institute
	Identity and Status Bureau, Estonian Police and Border Guard Board
Finland	National Police Board HQ
	National Police Board HQ, Police Operations Unit
	National Bureau of Investigation, Intelligence Unit
France	Criminal Intelligence Service of National Gendarmerie
	Forensic Institute of National Gendarmerie
	Central Directorate of Border Police
	Central Directorate of Judicial Police, National Division of Criminal Documentation and Coordination of Technical Police
Germany	Federal Police Headquarters, Department 3 – Counter Crime, Section 33
	Federal Criminal Police Office, Development and Quality Management Face Recognition
	Hessen State Criminal Police, Forensic Science Institute
	Bavarian State Criminal Police, Office of Criminal Investigation
Greece	Hellenic Police Forensic Science Division
	Hellenic National Passport and Secure Document Center
	State Security Division / Identity Cards & Archives Section of Hellenic Police Headquarters
Hungary	Ministry of Interior, Department for Schengen Matters & User Management
	Hungarian Institute for Forensic Sciences
	National Directorate-General for Aliens Policing
Italy	Carabinieri
	National Police
Latvia	Ministry of Interior, Information Centre
	Ministry of Interior, State Police
	Ministry of Interior, State Border Guard
	Ministry of Interior, Office of Citizenship and Migration Affairs
	Road Traffic Safety Directorate
	Ministry of Justice, Prison administration

Lithuania	Information Technology and Communications Department, Ministry of Interior
	State Enterprise Centre of Registers, Ministry of Justice
	Identity Documents Personalization Centre, Ministry of Interior
	State Enterprise REGITRA, Drivers Testing and Licencing Unit
Luxembourg	Grand Ducal Police
Malta	Malta Police Force
Netherlands	Centre for Biometrics, Dutch National Police
	National Vehicle Authority
Poland	Central Forensic Laboratory of the Polish Police
Portugal	Department of Civil Identification, Ministry of Justice
	Institute of Mobility and Transportation, Ministry of Infrastructure and Housing
	Forensic Laboratory of Judiciary Police
Romania	General Inspectorate of Romanian Police, National Forensic Institute
Slovakia	Division of Criminal Police Office, Presidium of Police Force
	Department of Informational Systems Management, Presidium of Police Force
	Department of Documents and Records, Presidium of Police Force
	Institute of Forensic Science, Presidium of Police Force
Slovenia	General Police Directorate, National Forensic Laboratory
	Ministry of Interior, Office for Administrative Internal Affairs and Naturalisation
Spain	National Police, Forensic Division
	National Police, Document Division
Sweden	Swedish Police Authority, National Forensic Centre
	Swedish Migration Agency
	Swedish Transport Agency
	Swedish Prison and Probation Service
Europol	European Counter Terrorism Centre
Interpol	Forensics and Police Data Management Sub-Directorate

Appendix 3: Facial recognition databases

Country/ Organisation	Database name	Database type	Database class	Software	Non-biometric information	Used for facial recognition	Database size	Person categories in database	Organisation involved
Facial recognition has been implemented									
Germany	INPOL	Criminal case management system	Criminal database	Self-developed	Yes	Yes	6.2 M individuals, 5.5 M mugshot images	Suspects, convicts, arrestees, wanted persons, missing persons and asylum seekers	Federal Criminal Police Office - maintainer of INPOL
France	Criminal Case History Database - TAJ	Criminal case management system	Criminal database	Self-developed	Yes	Yes	21 M individuals, 6 M facial images	Suspects and victims (i.e. unidentified dead bodies, seriously injured and missing persons)	Ministry of Interior - owner of TAJ
Italy	AFIS	Dedicated database to store and search fingerprints and facial images	Criminal database	Commercial	Yes	Yes	9 M individuals, 17 M facial images (10 M searchable)	Convicts, arrested suspects, unidentified persons, immigrants and asylum seekers	Forensic Institute, National Police - custodian of AFIS
Greece	Mugshot database	Dedicated database to store and search facial images	Criminal database	Commercial	No	Yes	377 000 individuals	Suspects who have been arrested and convicts who have been sentenced to imprisonment	Video and Image Laboratory of the Audiovisual Evidence of the Department of Photography and Modus Operandi of the Hellenic Police Forensic Science Division - custodian of the mugshot database
Slovenia	Record of photographed persons	Dedicated database to store and search facial images	Criminal database	Commercial	Yes	Yes	110 000 individuals	Suspects, missing persons and unidentified dead bodies	Slovenian Police - owner of the Record of photographed persons
Finland	Registered Persons Identifying Features database - RETU	Database containing mugshot images. RETU is a section of the National Criminal Database and it is searchable using FR system KASTU.	Criminal database	Self-developed	Yes, on the National Criminal Database	Yes	Not specified	Suspects	National Bureau of Investigation - custodian of KASTU
	Aliens database	Database containing information from foreigners. It is searcable using FR system KASTU.	Civil database	Self-developed	Yes	Yes, by limited number of police officers who have received special training	Not specified	Asylum seekers and aliens	Finnish Immigration Service - maintainer of Aliens database. National Bureau of Investigation - custodian of KASTU.
Austria	Criminal identification database - EDE	Database to store information needed for identification	Criminal database	Self-developed	Yes	Yes	620 000 known individuals, 1.25 M images	Criminals, missing persons and dead bodies	Federal Ministry of Interior - owner of the Criminal identification database
	Central register of foreigners - IRZ	Database to store information about foreigners	Civil database	Self-developed	Yes	No, although legally permitted	5 M datasets	Foreigners under different circumstances	Federal Ministry of Interior - owner of the Central register of foreigners
Netherlands	CATCH criminal	Physically separate database of the CATCH system that holds information derived during criminal proceedings	Criminal database	Self-developed database combined with commercial FR software	No	Yes	1.3 M individuals, 2.2 M images	Suspects and convicts	National Police - owner of the data in CATCH criminal. Centre for Biometrics - custodian and host of CATCH.
	CATCH alien	Physically separate database of the CATCH system that holds information derived from the core database for foreigners	Civil database	Self-developed database combined with commercial FR software	No	Yes, with a special permission	7 M individuals	Visa and asylum applicants	Directorate General Immigration - owner of the data in CATCH alien. Centre for Biometrics - custodian and host of CATCH.
Lithuania	Habitoscopic Data Register - HDR	IT system that stores information (including facial images) about the physical appearance of people	Criminal database	Self-developed	Yes	Yes	185 000 individuals, more than 400 000 facial images	Suspects, convicts, arrested persons, wanted persons, unidentified dead bodies and unidentified helpless persons	Information Technology and Communications Department under the Ministry of Interior - custodian of HDR

Country/ Organisation	Database name	Database type	Database class	Software	Non-biometric information	Used for facial recognition	Database size	Person categories in database	Organisation involved
Latvia	Biometric Data Processing System - BDAS	Central biometric repository to store facial and fingerprint data collected by state during various civil and criminal proceedings	Combined database of logically separated criminal and civil data	Commercial					Information Centre of the Ministry of Interior - owner and custodian of BDAS
	Criminal data array of BDAS	Sub-database of BDAS that stores information gathered during investigative activities	Criminal database	Commercial	Yes	Yes	270 000 cases of which 78 000 have facial images	Detained, suspected, accused and convicted individuals and unidentified dead bodies	
Hungary	Facial Image Registry	Central biometric repository (with FR search functionality) of facial images collected by the state during various document/civil proceedings. It is synchronised with several source databases where the biometric and non-biometric information is first entered.	Civil database	Commercial	No	Yes	30 M templates	Individuals of known identity from various document/civil proceedings	Ministry of Interior - responsible for the Facial Image Registry
UK	Police National Database - PND	Central national facial image database	Criminal database	Developed in conjunction with a commercial company	Not specified	Yes	14-16 M images	Detainees	Not specified
Europol	FACE	Dedicated database to store and search facial images	Criminal database	Self-developed	No	Yes	Not specified	Various groups of persons involved in a criminal procedure (e.g. suspects, victims etc.) as decided by Europol Member States and Third Parties	European Counter Terrorism Centre
	Not specified	Not specified	Not specified	Not specified	Not specified	Yes	Not specified	Not specified	European Cybercrime Centre
Interpol	Interpol Face Recognition System - IFRS	Dedicated database to store and search facial images	Criminal database	Commercial	Yes, limited amount	Yes	80 000 individuals	Wanted persons, missing persons and unidentified dead bodies sent by Interpol Member Countries	Interpol
Facial recognition implementation underway									
Sweden	ABIS	Multibiometric system to store and search fingerprints and facial images. In 2021, data stored on separate fingerprint and mugshot databases are expected to be merged into an ABIS system.	Criminal database	Commercial	Not specified	Use expected in 2021	Not specified	Not specified	National Forensic Centre - owner of data on ABIS
	Mugshot database	Dedicated database to store facial images that is without FR functionality	Criminal database	Self-developed	Yes	No	60 000 data entries	Suspects and convicts	National Forensic Centre - owner of data on mugshot database
Spain	ABIS	Multibiometric system to store and search fingerprints and facial images. Currently used AFIS for fingerprints will be converted into ABIS and populated with facial images stored in mugshot databases.	Criminal database	Commercial	Not specified	Use expected in 2021	Not specified	Not specified	Ministry of Interior -owner of ABIS
	Mugshot databases	Several separate dedicated databases to store facial images owned by different police forces. These databases are without FR search functionality.	Criminal database	Self-developed	Yes	No	3.9 M individuals, 5.6 M images	Arrestees	National Police, Guardia Civil and Regional Police - owners of mugshot databases

Country/ Organisation	Database name	Database type	Database class	Software	Non-biometric information	Used for facial recognition	Database size	Person categories in database	Organisation involved
Romania	National Biometric Identification System - NBIS	Dedicated database to store and search facial images that is currently without FR search functionality	Criminal database	Self-developed	Yes	Use expected in 2021	300 000 individuals with an expected increase by 500 000 individuals	Suspects, convicts, unknown persons, missing persons and unidentified dead bodies	Romanian Police - owner and custodian of NBIS
Czech Republic	Central Biometric Information System - CBIS	Multibiometric system to store and search fingerprints and facial images. CBIS is under development and will be populated with facial images from FODAGEN database.	Criminal database	Commercial	Not specified	Use expected in 2021	Not specified	Not specified	Police of Czech Republic - responsible for facial recognition implementation
	FODAGEN	Dedicated database to store fingerprints and facial images that is without FR search functionality	Criminal database	Self-developed	Yes	No	200 000-300 000 records from individuals	Suspected, accused and convicted persons	Police of Czech Republic - owner of FODAGEN
Cyprus	ISIS Faces	Dedicated database to store and search facial images that is currently without FR search functionality	Criminal database	Commercial	Yes	Use expected in 2021-2022	2000 individuals	Convicts	Criminalistic Services of Cyprus Police - owner of ISIS Faces
Estonia	ABIS	Multibiometric system to store and search fingerprints and facial images from both criminal and civil proceedings. The criminal part of ABIS is expected to be launced in March 2021 and the facial modality of the criminal part is expected to be functional in 2022.	Combined database of logically separated criminal and civil data	Commercial	Yes	Use expected in 2022	No images yet	Suspected, accused and convicted persons	Ministry of Interior - owner of ABIS
Croatia	ABIS	Multibiometric system to store and search fingerprints and facial images that is currently without FR search functionality.	Criminal database	Commercial	Yes	Use expected in 2021	220 000 individuals	Suspects and offenders	Ministry of Interior - owner of ABIS
	Image repository of civil documents	Central repository for storing facial images collected during issuing of ID cards, travel documents and driver's licences. Database is in use, but currently without FR search functionality.	Civil database	Self-developed	Not specified	Use expected in 2021	5.7 M individuals, 18 M images	Applicants of ID cards, travel documents and driver's licences	Ministry of Interior - owner of Image repository of civil documents

Appendix 4: Image requirements

Country/ organisation	Database name	Database class	Types of images	Quality requirements	Standard operating procedures (SOPs)	Training	Quality control	File format
Facial recognition has been implemented								
Germany	INPOL	Criminal database	Front, both sides, two 45-degree images and full body image	Images are stored in accordance with ISO standard 19794-5	SOPs for image captrue	Officers are provided with specific training both in the recording of fingerprints and facial images	Officer that performs the enrolment is required to check that the image is in accordance with SOPs	JPEG
France	Criminal Case History Database - TAJ	Criminal database	Front, right side, left half-side and full body from the front	Requirements are set to many parameters including pose, distance, background and lighting. For FR searches, the distance between the pupils must be at least 150 pixels.	Witten guidelines for capturing of controlled facial images and written recommendations for entering the image to the database	Personnel are trained for image enrolment	Quality of the images is assessed by the FR algorithm	JPEG (preferred), PNG, BMP, GIF
Italy	AFIS	Criminal database	Front and right side	No quality standard is currently used	There are no written instructions	Personnel are trained to capture images	It is planned to implement an automatic quality check at the capture stage	JPEG
Greece	Mugshot database	Criminal database	Front, right side and full body image	Not specified	Written instructions for image capture	Individuals performing enrolment have been trained by the company that provided the facial recognition system	Not specified	JPEG
Slovenia	Record of photographed persons	Criminal database	Front, right side, left half-side and images of tattoos	Not specified	1) Procedure for photographing of suspects, 2) Enrolment of images, 3) Using of Face Trace module and performing FR searches	No special training is provided	Not specified	JPEG
Finland	Registered Persons Identifying Features database - RETU	Criminal database	Front, right side, left side, front quarter side right, front quarter side left, back quarter side right, back quarter side left and full body front	Not specified	Not specified	Not specified	Not specified	Not specified
Austria	Criminal identification database - EDE	Criminal database	Front, right side, left half-side, full body, special features and tattoos	At least 32 pixels between the centres of the eyes in order to perform a FR search, the resolution of images is 960 x 1280 pixels	Best practice manual is issued to police officers collecting biometric data and it is called 'Provision for Biometric Identification'	All police officers who take photographs have undergone special training for the collection of biometric data	Quality checks of the photographs taken are performed centrally in the Criminal Intelligence Service of the police	Not specified
Netherlands	CATCH criminal	Criminal database	Front, only in rare cases other views may be taken	Requirements are set for images to be used for searches: at least 40 pixels between the eyes, both eyes visible, good sharpness, even lighting, neutral expression	SOP for data aquisition following ISO 19794	All police officers who take photographs have undergone basic training for the collection of biometric data	Not specified	JPEG, PNG, BMP
Lithuania	Habitoscopic Data Register - HDR	Criminal database	Front	Recommendations – frontal view image looking directly and a yaw angle (left or right), a pitch angle (up or down) and a roll angle (facial tilt) deviation from the direct view should be +/-15 degrees. Probe images that are searched against the database images should have at last 20 pixels distance between the eyes. Controlled images against which searches are performed should have 80-120 pixels distance between the eyes.	There are no written methods for the capture and enrolment of facial images	No regular training program is in place	Images used for facial recognition must comply with the requirements set by the manufacturer of the FR software	JPEG, PNG, BMP

Country/ organisation	Database name	Database class	Types of images	Quality requirements	Standard operating procedures (SOPs)	Training	Quality control	File format
Latvia	Criminal data array of BDAS	Criminal database	Front	Facial images must correspond to the requirements of ANSI/NIST ITL-1:2011 and ISO/IEC 19794-5 Part 5: Face image data	Written instructions are provided to the personnel that capture facial images	Not specified	Built-in quality assessment tool checks the quality of images and their compliance with the minimum requirements set in the system	Not specified
Hungary	Facial Image Registry	Civil database	Front	All photographs are taken in accordance with ICAO and ISO/IEC 19794-5 standards	Written document ´A Methodical Guide on the Technical Equipment to Use in the Document Office and the Requirements for Portrait Photography´ is in use for the capturing and enrolment of images	Training of personnel working with equipment that is used for image capturing, and software that is used for databasing	Not specified	JPEG
Europol	FACE	Criminal database	Front, both sides and both ¾ sides	Europol has no direct influence on the image quality	Not applicable	Europol officials who enter facial images in FACE are accredited to carry out this task and must have received minimum training	Quality assessment of images follows the fundamentals of the ACE-V workflow as described within the ENFSI Best Practice Manual for Facial Image Comparisons	JPEG, PNG, GIF
Interpol	Interpol Face Recognition System - IFRS	Criminal database	Front	All the images that are stored in IFRS must be compliant with the requirement of having 40 pixels between the centres of the eyes	Interpol has produced a guideline ´INTERPOL Facial Images Best Practices Guide´ for support purposes. A written standard operating procedure is used for the entry of images to database.	Interpol officers that enter facial images in IFRS have undergone on-the-job training	To ensure compliance, images undergo a manual control before being entered into the database. In addition, IFRS includes specific software ASTEK that is used for the quality control.	JPEG, PNG, BMP, TIFF
Facial recognition implementation underway								
Sweden	Mugshot database	Criminal database	Front, right side, left side, full body front, right and left and special marks	Frontal face images are of resolution 300 x 400 pixels	Written SOP regarding the capture of fingerprints and mugshots	Police officers receive training to achieve a licence for the capturing of fingerprints and mugshots. Training is also provided for the enrolment procedure, together with written training materials.	Not specified	JPEG
Spain	Mugshot databases	Criminal database	Front, right and left side, semi-left side (some districts also have semi-right side), full body frontal, marks, scars and tattoos	The minimum image size and resolution requirements are 2 Mb and at least 300 PPI, respectively.	Not specified	Police officers acquiring mugshot data have recived a special training, of which one week is dedicated to capturing of mugshots	There is no automatic quality control in place	JPEG
Romania	National Biometric Identification System - NBIS	Criminal database	Front, right side, left side, full body frontal, special marks, scars and tattoos	Facial images are captured according to ICAO 19303 and ISO 19794 standards	SOP has been developed for the capture and enrolment of images	Training is provided to forensic examiners who capture and enrol images	Not specified	PNG
Czech Republic	FODAGEN	Criminal database	Front, right side, left half-side, full body, special marks and tattoos	Internal quality requirements that are for the most part in accordance with the ICAO standard	Internal regulations for personnel capturing facial images	Training is provided during special courses for police officers performing facial image capture	Not specified	JPEG, JPEG/JFIF
Cyprus	ISIS Faces	Criminal database	Front, side views and 45-degree views	Not specified	Not specified	Not specified	Not specified	JPEG

Country/ organisation	Database name	Database class	Types of images	Quality requirements	Standard operating procedures (SOPs)	Training	Quality control	File format
Estonia	ABIS	Combined database of logically separated criminal and civil data	To be decided	Not in place	Not in place	Not in place	Not in place	To be decided
Croatia	ABIS	Criminal database	Front, right side and left half-side	Not specified	Photographs are taken in accordance with an internal guideline known as a ´Rulebook on fingerprinting and photographing persons´.	Criminalistic technicians of the Croatian Police are trained in facial image capture. The forensic technicians of FSC have been trained in image enrolment.	Quality of an image is checked by the person capturing the image	JPEG

Appendix 5: Facial recognition searches

Country/ Organisation	Database name	Facial recognition searches started	Search engine	Type of controlled image searched	Persons who perform facial recognition searches	Number of persons performing FR searches	Number of posts in the candidate list	Can the same candidate appear in the candidate list more than once?
Germany	INPOL	2008	Cognitec Face VACS	Frontal	Trained facial examiners and experts at all three levels of German policing. Only qualified facial image examiners/experts are permitted to conduct FR searches.	70	10, 20 or 100, can be increased to 1000	Yes. List may include more than one image for a given individual.
France	TAJ	2013	Cognitec Face VACS DBScan	Frontal	Investigators of National Gendarmerie and National Police	Exact number is not known, but it is large	Maximum of 200, depending on the number of candidates above a set threshold	Yes. List may include more than one image for a given individual.
Italy	AFIS	2017	NeoFace Watch from NEC and software from Reco. It is possible for the user to select which of the two search engines to use.	Frontal	Police officers of National Police and Carabinieri, and forensic experts	Exact number is not known, but it is large	50	No. If the same person exists as several entries in the database, the software can group all these as one single candidate in the search result, which is ranked according to its highest score value.
Greece	Mugshot database	2019	Fire Exos II from Unidas	Frontal	Facial examiners of the Video and Image Laboratory	4	Set by the examiner	Not specified
Slovenia	Record of photographed persons	2015	VeriLook from Neurotechnology	Frontal	15 police officers at the regional level and 2 police officers at the state level	17	51	Not specified
Finland	RETU and Aliens databases searched with facial recognition system KASTU	2020	Commercial, vendor not specified	Not specified	Law enforcement officers, border guards and customs officers officers who require it in relation to their duties, while permission to search Aliens database is granted only to officers that have received a special training.	Exact number is not known, but it is large	Maximum of 200	Not specified

Country/ Organisation	Database name	Facial recognition searches started	Search engine	Type of controlled image searched	Persons who perform facial recognition searches	Number of persons performing FR searches	Number of posts in the candidate list	Can the same candidate appear in the candidate list more than once?
Austria	EDE	2020	Cognitec	Frontal and half-side images	Qualified specialists of the Criminal Intelligence Service	3	30 with the 10 highest ranking candidates forwarded to the investigating officer	No
Netherlands	CATCH criminal and CATCH alien	2016	Face Expert from Idemia	Frontal	Facial experts at the Centre for Biometrics (24/7 service)	30	Maximum of 50	Not specified
Lithuania	HDR	2019	NeoFace Watch from NEC	Frontal	Police officers and forensic experts to whom access to HDR FR module has been granted	More than 500	Set by the user	Not specified
Latvia	Criminal data array of BDAS	2012	MorphoTrust ABIS Search Engine	Frontal	A wide range of persons working for law enforcement are allowed to perform FR searches	Exact number is not known, but it is large	Not specified	Not specified
Hungary	Facial Image Registry	2016	NEC	Frontal	Analysts of the Hungarian Institute for Forensic Sciences	27	1000 as a rule. Can be changed by the analyst depending on specific case.	Yes. List may include more than one image for a given individual.
Europol	FACE	2017	Developed in-house, based on open-source components	Not specified	Europol officials of the European Counter Terrorism Centre	Not specified	10, 50, 100 or 200. Can be selected by the official performing the search.	Not specified
Interpol	IFRS	2016	Morpho Face Investigate from Idemia	Frontal	Interpol officers	4	Not specified	No. Only one image per person (the most likely one) appears in the list based on a decision made by the algorithm.

Country/ Organisation	How facial recognition search results can be used?	Number of searches	Number of matches	Match rate	Training	Standards/ written instructions	Proficiency monitoring
Germany	Primarily for criminal intelligence purposes. However, in certain circumstances FR search results can be used as evidence in court.	53 000 in 2019	2 200 in 2019	4.15%	Examiners have undergone an 11-week training programme and are trained in performing FR and facial image comparisons. Experts are examiners with an additional qualification in presenting the findings in court. Experts have to complete a two and a half to three-year training programme including courses and exams.	Not specified	Only 1:1 facial image comparison proficiency testing (national and ENFSI tests)
France	For operational purposes to support the investigation. The search results are not suitable to be presented as evidence in court.	200 000 in 2018	Not specified	Not specified	Some basic training is provided to the investigators of the National Police and the National Gendarmerie who are using the TAJ FR search functionality. However, no systematic training is compulsory.	No specific written methods have been developed for conducting FR searches	There is no proficiency monitoring
Italy	For criminal intelligence purposes. In general, the FR search results cannot be used in court, but only 1:1 facial image comparison reports provided by the forensic services.	Not specified	Not specified	Not specified	There is basic training available for operators on how to use the FR software, including some insights into how the results can be used and when to ask for a forensic 1:1 facial image comparison.	Not specified	Only 1:1 facial image comparison forensic experts participate in proficiency testing (ENFSI test)
Greece	Primarily used for investigative purposes, but the results can also be used in court as evidence, if needed.	Not specified	Not specified	Not specified	Forensic examiners were trained by the company that provided the FR software	No written instructions are in place for FR searches	Not specified
Slovenia	Results are used as an investigative lead. In order to use the search result as evidence in court, a manual 1:1 comparison must be performed and a relevant report prepared.	150-200 per year	2-3 per year	Around 1%	Not specified	Written document 'Using of Face Trace module and performing facial recognition searches'	Not specified
Finland	FR system is used as a criminal intelligence tool and search reports are not regarded to be of evidential value in the Finnish court system.	Not specified	Not specified	Not specified	Before a law enforcement officer can perform a search on the KASTU system he/she is required to complete an online training course. Access to the Alien’s database requires attendance to additional classroom-based training.	There is a brief guideline in place in relation to FR searches	Not specified

Country/ Organisation	How facial recognition search results can be used?	Number of searches	Number of matches	Match rate	Training	Standards/ written instructions	Proficiency monitoring
Austria	Search results can only be used for investigative purposes.	Not specified	Not specified	Not specified	Not specified	Not specified	Not specified
Netherlands	Result is reported as an investigational lead. Whether this information is added to the evidence and presented in a court is decided by the public prosecutor.	1048 in 2018	86 in 2018	8.2%	One week training followed by at least 3 month on the job training	No written instructions are in place for FR searches	There is no proficiency monitoring
Lithuania	FR search results are not used as evidence in court.	Not specified	Not specified	Not specified	Training was provided to 10 persons by the company that provided software. Most of the persons that can perform FR searces have not received a special training.	No written instructions are in place for FR searches	There is no proficiency monitoring
Latvia	Search results can only be used for intelligence and operative purposes and cannot be used in court.	Not specified	Not specified	Not specified	Training for FR searches is provided, on demand, for persons performing this activity	An internal written document	There is no proficiency monitoring
Hungary	FR search results are used only as an investigative lead and they cannot be used as evidence in court.	Not specified	Not specified	Not specified	There is a training in place for personnel performing FR searches	Not specified	Not specified
Europol	FR search results are meant to be used for intelligence and not as evidence in court.	Not specified	Not specified	Not specified	Europol officials who enter facial images in FACE and perform FR searches are accredited to carry out these tasks and must have received minimum training in facial comparison and identification	An internal written guideline has been developed	Not specified
Interpol	FR search results are to be used only as investigative leads and not as evidence in court.	Not specified	Around 300 annually	Not specified	Officers who perform FR searches have been trained by the FBI on facial comparison and must have at least two years of work experience in the FR field before being recruited by Interpol	A written SOP is available for FR searches	Only 1:1 facial image comparison proficiency testing (ENFSI test)

Appendix 6: Use of non-criminal data

Country/ Organisation	Database name	Database class	Is database facial recognition searchable?	Are images of missing persons included into the database?	Are images of unidentified dead bodies included into the database?	Are images of foreigners included into the database?	How data in other civil register can be used?
Facial recognition has been implemented							
Germany	INPOL	Criminal database	Yes	Yes		Asylum seekers, stored separately from the criminal database	Searching facial images that have been recorded for civil purposes, such as driving licences, passport applications, is neither technically possible, with current infrastructure, nor is it legally permitted for police forces. However, in exceptional circumstances, police forces are permitted to ask for access to an image in such a database, for a 1:1 examination to establish the identity of an individual.
France	TAJ	Criminal database	Yes	Yes	Yes		With the current technical infrastructure and legal landscape, it is not possible for the police to search facial images that have been recorded for civil purposes, such as applications for driving licences, passports etc. Only in very exceptional circumstances, are the police permitted to ask for such images for a 1:1 examination.
Italy	AFIS	Criminal database	Yes			Asylum seekers and immigrants. 90% of the AFIS subjects are foreigners.	Police can ask for the image of a person of interest from another database (including civil databases) for manual 1:1 facial image comparison, but it is not allowed to perform FR searches in civil databases for the purpose of criminal investigations.
Greece	Mugshot database	Criminal database	Yes				Facial images that are collected and stored for civil purposes (i.e. in the course of various document applications) cannot be used for FR in criminal investigations. However, the police can request such an image for a manual 1:1 comparison.
Slovenia	Record of photographed persons	Criminal database	Yes	Yes	Yes		It is permissible, for the images in civil databases (from applicants for passports and identity cards) to be accessed by the police during criminal investigations, but the civil databases are not FR searchable.
Finland	RETU	Criminal database	Yes				Legally it is not allowed to use the data collected during civil document proceedings in criminal investigations. Currently the passports department is constructing a facial comparison system with the goal of preventing the registration of double identities, but it will not be available to the police in relation to criminal activity. However, it will be available for use in the identification of unknown deceased individuals.
	Aliens database	Civil database	Yes, but additional training and permissions are required before an individual can search the Aliens database			Data on asylum seekers and other non-Finnish citizens	
Austria	EDE	Criminal database	Yes	Yes	Yes, but facial recognition searches for identification purposes are not performed		It is not permitted to perform FR searches for crime investigation in other civil databases such as in the Identity documents register, the Social security register and the Driver's licence database. Nevertheless, the police can request images from these databases.
	IRZ	Civil database	Legally allowed, but technically not possible			Foreigners under different circumstances	
Netherlands	CATCH criminal	Criminal database	Yes				In general, it is not permissible to perform FR searches for criminal investigation purposes in the municipal identity document registers nor in the driver's licence database. However, on special request by the public prosecutor, searches can be performed. Nevertheless, at the present time, FR searches in the civil databases are not technically possible.
	CATCH alien	Civil database	Yes, but searches are only permitted with a written order from the prosecutor and with the consent of a judge			Visa and asylum applicants	
Lithuania	HDR	Criminal database	Yes		Yes	Foreigners detained for illegal trespassing at the state border	Regarding facial images of civil origin (i.e. from various document proceedings), it is permissible for law enforcement to use such images for manual 1:1 comparisons or 1:N searches against HDR. An automated search capability with the current infrastructure is neither permitted nor technically possible within civil databases.

Country/ Organisation	Database name	Database class	Is database facial recognition searchable?	Are images of missing persons included into the database?	Are images of unidentified dead bodies included into the database?	Are images of foreigners included into the database?	How data in other civil register can be used?
Latvia	Criminal data array of BDAS	Criminal database	Yes		Yes		Only information in the criminal data array of BDAS is used for FR searches during crime investigations, while all other sub-databases of BDAS are unavailable for the crime investigation because of both technical and legal restrictions.
	Non-criminal data arrays of BDAS	Civil database	No			Yes	
Hungary	Facial Image Registry	Civil database	Yes			Yes	The data sources for the Facial Image Registry are databases that contain facial images of individuals of known identity from various document/civil proceedings and they can be searched during criminal investigation.
Facial recognition implementation underway							
Sweden	ABIS	Criminal database	Yes, after FR implementation is finished				The police are allowed to use an image of a person of interest from other databases, including civil databases. It is not allowed to perform a FR search in civil databases for the purpose of criminal investigations.
Spain	ABIS	Criminal database	Yes, after FR implementation is finished				The police can request facial images from civil databases for 1:1 comparisons, but not for use with FR searches.
Romania	NBIS	Criminal database	Yes, after FR implementation is finished	Yes	Yes		For 1:1 comparisons, the police are permitted to use photographs from civilian applications.
Czech Republic	CBIS	Criminal database	Yes, after FR implementation is finished				The Law on Police of Czech Republic adopted in 2019 permits the use of images in civil databases for FR searches in criminal investigations, but it is not technically possible at the present time.
Cyprus	ISIS Faces	Criminal database	Yes, after FR implementation is finished				Not specified
Estonia	ABIS - criminal subsystem	Criminal database	Yes, after FR implementation is finished				The Estonian legal framework currently allows the civil fingerprint database to be accessed for solving the most serious crimes, and the same principle will probably be applied for facial images.
	ABIS - civil subsystem	Civil database	Yes, after FR implementation is finished				
Croatia	ABIS	Criminal database	Yes, after FR implementation is finished				After implementation of FR the information in civil document databases will be available for 1:N searches in criminal investigations and in the search for missing persons.
	Image repository of civil documents	Civil database	Yes, after FR implementation is finished				

Appendix 7: Uncontrolled images

Country /organisation	Uncontrolled images
Facial recognition has been implemented	
Germany	Uncontrolled images (e. g. images from CCTV cameras) may be stored in the INPOL database if these images are the only ones available.
France	TAJ is also used for storing uncontrolled images (e.g. photo robot sketches, surveillance images etc.). The number of uncontrolled facial images was approximately 6000 out of 6 M images as of October 2019.
Italy	Uncontrolled images are not stored in the AFIS facial image database.
Greece	Uncontrolled images are not stored in the mugshot database.
Slovenia	From November 2020, uncontrolled images (e.g. images obtained from surveillance cameras) are entered and stored in the Record of photographed persons.
Finland	Uncontrolled images are not stored in the National criminal database.
Austria	EDE includes crime scene images. The number of uncontrolled images as of September 2019 was less than 1000.
Netherlands	Currently, uncontrolled images are not stored. However, plans exist to start storing such images in the future.
Lithuania	Uncontrolled images are not stored in HDR, but in a crime scene register "*Iniciativa*".
Latvia	Uncontrolled facial images are not stored in the criminal array of BDAS.
Hungary	Uncontrolled images related to criminal activity (e.g. CCTV camera footage) are not stored in any database.
Europol	FACE is used for storing of both controlled and uncontrolled facial images. It is also populated with uncontrolled facial images that are extracted from propaganda and other relevant materials stored in the Europol Check-the-Web portal.
Interpol	Uncontrolled images (e.g. from CCTV) are also submitted for storage in the database. However, such images do not often meet the quality requirements for storage and, typically, are only searched against the IFRS.
Facial recognition implementation underway	
Sweden	Currently, uncontrolled images are not stored in any database. These images are only archived in the relevant investigative case records. Nevertheless, the aim of National Forensic Centre is to create a database of uncontrolled images for unsolved crimes (similar to the latent fingerprint database) but, before that is initiated, a legal analysis will need to take place and additional/updated legislation may need to be introduced.
Spain	Unidentified offenders captured on imagery, such as CCTV or fake documents, are stored in database at the investigation unit of the National Police. There are about 50 000 images in this database, but there might also be similar smaller databases in regional police forces. Currently, there is no plan to include the database of uncontrolled images into the FR system.
Romania	At this time, uncontrolled images are not stored in NBIS. However, there are plans to store such images in NBIS in the future.
Czech Republic	There are discussions as to whether uncontrolled images should be included to CBIS.
Cyprus	No uncontrolled images are stored in ISIS Faces database.
Estonia	No decision has been made in regard to uncontrolled images.