MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE

MAY 2022

PART 2

CLASSIFICATION

Authors:

Theodore CHRISTAKIS (project leader)
Karine BANNELIER
Claude CASTELLUCCIA
Daniel LE METAYER

With contributions from:

Alexandre LODIE
Stephanie CELIS JUAREZ
Coralie PISON-HINDAWI
Anaïs TROTRY

AI-REGULATION.COM

MIAI Grenoble Alpes

AUTHORS BIO

Theodore CHRISTAKIS is Professor of Law at University Grenoble Alpes, director of research for Europe with the Cross-Border Data Forum, Senior Fellow with the Future of Privacy Forum and a former Distinguished Visiting Fellow at the New York University Cybersecurity Centre. He is director of the Chair on the Legal and Regulatory Implications of Artificial Intelligence with the Multidisciplinary Institute on AI (AI-Regulation.com). He has been a member of the French National Digital Council, and he is currently serving as a member of the French National Committee on Digital Ethics and of the International Data Transfers Experts Council of the UK Government.

Karine BANNELIER is Associate Professor of International Law at University Grenoble Alpes. She is deputy director of the Chair of the Legal and Regulatory Implications of Artificial Intelligence at the Multidisciplinary Institute on AI, director of the Grenoble Alpes Cybersecurity Institute and Senior Fellow on Cybercrime at the Cross Border Data Forum. She has served as an expert on cybersecurity issues for French governmental agencies and for international organisations.

Claude CASTELLUCCIA is research director at Inria (France) and a founding member of the Privatics team (models, architectures and tools for the protection of privacy in the information society) where he is conducting research in the areas of digital privacy protection and computer security. He is also the scientific director of the Chair on the Legal and Regulatory Implications of Artificial Intelligence at the University Grenoble Alpes and a member of the French Data Protection Agency (CNIL).*

Daniel LE MÉTAYER is an independent consultant. Until January 2022, he was Research Director at Inria in the team Privatics working in the area of privacy protection, in particular privacy by design, privacy risk analysis, accountability and transparency. He has also been a member of the Commission of the French National Assembly on the rights and freedoms in the digital society and chairman of the scientific committee of the CNIL-Inria Privacy Award.

Other Contributors bio

Alexandre LODIE has joined the Chair as a Research Fellow in September 2021. He has successfully defended a PhD thesis on the principle of non-interference in the context of the Cyberspace development in December 2021. He has also taught law at University Grenoble Alpes and University Savoie Mont-Blanc for four years (2017-2021).

Stephanie CELIS JUAREZ has joined the Chair as a Research Fellow in October 2021. She worked as a lawyer in diverse law branches (civil, administrative, constitutional) in her native country, Mexico. She is particularly interested in online political manipulation and international security and politics.

Coralie PISON HINDAWI has recently joined the Chair as a Research Fellow. Prior to that, she was for many years Associate Professor in International Politics at the American University of Beirut, where she focused on arms control as well as ethics in international affairs. She is associate editor of the journal *Critical Studies on Security*.

Anaïs TROTRY is currently a PhD candidate at University Grenoble Alpes (UGA). Under the supervision of Professor Christakis, her thesis focuses on the concept of risk and on its role in the regulation of new technologies (AI, cyber, access to data and data protection). She is affiliated with the Chair and she has been participating in its work since September 2020.

Acknowledgments and Disclaimers

This is the first report, in a series of six, of a research project that began in June 2021 and covers developments up to April 2022.

The authors would like to thank all of those who have contributed ideas and comments over the various stages of this research project. Special thanks for their peer-review of a previous version of this report (all errors are ours): Professor Peter Fussey, University of Essex, Human Rights, Big Data and Technology Project; Irina Orssich, Head of Sector AI Policy, European Commission DG Communications Networks, Content and Technology; Isabelle Hupont-Torres and Emilia Gomez-Gutierrez, European Commission Joint Research Centre (JRC).

Many thanks also to Andy Brinded, copyeditor at Ableword (UK), for linguistic proof-reading, Gilles Esparbet for the composition of the cover and Jonathan Collin of Cerf à Lunettes for the images in our classification table. Thanks also to Mathias Becuywe and Maeva El Bouchikhi for their assistance during the initial stage of this project.

This work has been supported by MIAI@Grenoble Alpes, (ANR-19-P3IA-0003). It has also been supported by the Future of Privacy Forum.

The statements in this report are attributable to the authors only, and this publication does not necessarily reflect the views of the Future of Privacy Forum, the Multidisciplinary Institute of Artificial Intelligence, other members of the AI-Regulation Chair or any other partner organisation of the Chair or to which the authors are affiliated.

* The work presented in these reports started before Claude Castelluccia was nominated as a member of the CNIL in August 2021 and was performed at Inria and MIAI, independently of his activity at the CNIL. The views and opinions expressed in this document do not necessarily reflect the position of the CNIL.

TABLE OF CONTENTS

Mapping the Use of Facial Recognition in Public Spaces in Europe

Part 2

CLASSIFICATION

Authors:

Theodore CHRISTAKIS (project leader)

Karine BANNELIER

Claude CASTELLUCCIA

Daniel LE MÉTAYER

With contributions from:

Alexandre LODIE

Stephanie CELIS JUAREZ

Coralie PISON-HINDAWI

Anaïs TROTRY

EXECUTIVE SUMMARY

In Part 1 of our "**MAP**ping the use of **F**acial **R**ecognition in public spaces in **E**urope" (MAPFRE) project we explained in detail what "facial recognition" means, addressed the issues surrounding definitions, presented the political landscape and set out the exact material and geographical scope of the study. Furthermore, we explained how our study covers all the ways in which face processing systems are used in public spaces in Europe, whether the data involved are "biometric data" or, to use the new term, are "biometrics-based data". Drawing on the draft EU AI Regulation, we also precisely defined what we mean by the term "public spaces" and presented three subcategories, that we have used for our study: "open spaces"; "restricted spaces"; "closed spaces".

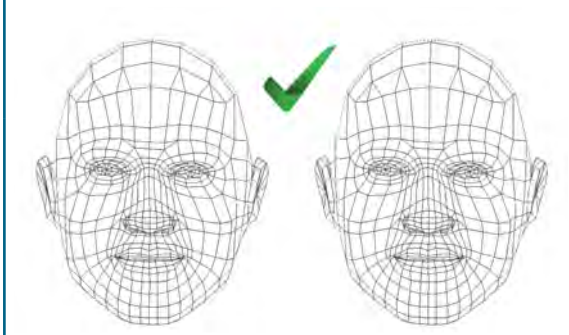
As noted by the French Data Protection Authority, CNIL, **"the current debate on facial recognition is sometimes distorted by a poor grasp of this technology and how it exactly works"**. The specific objective of the present paper is to present how facial recognition and facial analysis work.

We have also endeavoured to produce a **"Classification Table"** detailing how facial recognition/analysis is used in public spaces. This classification table tries to present in the most accurate and accessible way the different facial processing functionalities and applications used in public spaces, which encompass the various forms of both "face recognition" and "face analysis".

We hope that this classification table, together with the illustrations, explanations and numerous examples that are included, which are based on our "25 selected case studies", will serve as a useful tool in preventing the various uses of facial recognition being conflated, and will bring further nuance and clarity to the public debate.

MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE

Classifying the uses of facial recognition/analysis in public spaces

FUNCTIONALITY	APPLICATION	CAPTURED FACES	REFERENCE FACES	EXPLANATION	EXAMPLES
1. FACE VERIFICATION					
	Authorisation using a biometric token	1	1	Compares a single face against a reference image stored in a biometric token of the user (e.g. a passport). Face recognition is used to confirm that there is indeed a match between the two images. This may be used in security access control protocols.	PARAFE Automated Passport control at the border (FR)
	Authorisation using an ID token	1	1(in M)	Compares a single face against a single reference indexed in a database. A token stores an identifier of the user. The token can be in the form of a badge, QR code in a smartphone, etc. It is provided as an input by a person and links to his/her specific image stored in this database "1(in M)". Face recognition is used to confirm that there is indeed a match between the two images. This may be used for instance in access controls in a closed space (e.g a school).	PACA Schools Access Control in High schools in the South of France
2. FACE IDENTIFICATION					
Individual Identification/Face Search (1-M)					
	Individual Identification	1	M	Tries to identify a person for which a face picture is available and relies on a database of face images associated with identities. Mostly used for public security purposes (e.g. by the police to identify suspects in criminal investigations) .	TAJ (FR), SARI Enterprise (IT), South Wales Police (UK), Clearview, Olympic Stadium (IT)
	Authorisation without using a token	1	M	Authorises a user by searching if his faceprint appears in a database of authorised users.	Molenbeek Stadium (BE), MONA App in Airports (FR), Aena/ Iberia (ES), Payments in School Canteens (UK) (...)
Large Scale Face Matching					
	Surveillance of an Open or Restricted Public Place	N	M (or 1)	Monitors a public place (the entrance to a stadium, a crowd attending a specific event, the streets of a city, etc.) to identify people in a database (e.g. used by the police or private security firms to identify people in a watchlist). Can also be used to search for a missing child in a public place (in this case M=1).	South Wales Police (UK), London MPS (UK), Mercadona Supermarkets (ES), Brondby IF (DK), Zaventem Airport (BE), SARI Real Time (IT) (...)
Targeted Face Tracking					
	Targeted Face Tracking	N	1 (or M)	Tracks an individual (or several individuals) using video cameras in a geographic zone (for example to track where a suspect is moving in a city).	Trial proposed during Nice Carnival (FR) or phase 2 in Berlin Station (DE)
3. FACE ANALYSIS					
	Categorisation, Emotion Recognition	1 or N		Tries to infer specific attributes from faces (e.g. emotions, signs that the person may be lying, gender, their estimated age, whether a person is wearing a mask at a train station, etc.).	iBorderCtrl project (HU, GR and LV) Datakalab (FR)

INTRODUCTION

In Part 1 of our "**MAP**ping the use of **F**acial **R**ecognition in public spaces in **E**urope" (MAPFRE) project[1] we explained in detail what "facial recognition" means, dealt with issues of definition, and set out the exact material and geographical scope of this study. We further explained how our study covers all uses of face processing systems in public spaces in Europe, whether the data involved are "biometric data" or, to use the new term, "biometrics-based data". However, our study does not concern situations in which neither "face recognition" nor "face analysis" is taking place, such as general video surveillance or "biometrics-based data" processing that doesn't involve face processing (such as voice, gait or behavioural recognition not based in facial analytics). Drawing on the draft EU AI Regulation, we have also defined with precision how we use the term "public spaces" and presented three subcategories, that we have used for our study: "open spaces"; "restricted spaces"; closed spaces.

As noted by the French Data Protection Authority (DPA), "*Commission Nationale de l'Informatique et des Libertés*" (CNIL) in November 2019, **"the current debate on facial recognition is sometimes distorted by a poor grasp of this technology and how it exactly works"**.[2] The objective of the present paper is, precisely, to present, in the most accessible way possible, exactly how facial recognition and facial analysis work. We have also endeavoured to produce a **"Classification Table"** detailing the uses of facial recognition/analysis in public spaces. This classification table tries to present in the most accurate and accessible way the different facial processing functionalities and applications used in public spaces, which encompass the various forms of both "face recognition" and "face analysis". We hope that this classification table, together with the illustrations, explanations and examples that are included, will become a useful tool to prevent the phenomenon of conflating diverse uses of facial recognition together and to bring further nuance and precision to the public debate, which was highlighted by the CNIL.

Before jumping to the end of this paper, where the classification table and its illustrations are presented, we invite readers to look at our explanations of what "facial processing" means and how it works, as well as what constitutes the purposes of facial processing systems and the differences between the *functionalities* and *purposes* of such systems.

---

[1] See T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term", Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

[2] CNIL, "Facial Recognition: For a Debate Living up to the Challenges", November 15, 2019. Translation and emphasis by the CNIL.

UNDERSTANDING HOW FACIAL PROCESSING WORKS

It is important to note that a Facial Recognition (FR) application, is comprised of an FR system, which drives the technical components, but also an *operational* element that includes the management procedures used by human operators.

Furthermore, an FR system is itself composed of a ***Facial Processing component*** ("FPC"), whose inputs come from a pre-processing phase (for example the phase that captures and pre-processes the images), and whose outputs are post-processed to fulfil the FR system's *purpose* (or *finality*).

For example, an FR-based *authorisation application* (such as a system for crossing a security control equipped with a biometric authentication system in order to access a building[3]) could involve the following 3 phases (pictured in Figure 1):

- The *pre-processing* phase, the inputs of which come from the badge of a user and an image captured by a camera. These inputs are processed to output a pre-processed image and an identity ID (obtained by a badge reader).
- A *face verification* component that uses the pre-processed image and user's ID to check whether the user's face is similar to the one registered in the system for the user with the ID (as this will be detailed later, this face verification phase typically involves the extraction of biometric templates). This phase outputs the ID together with the value "1" or "0" according to whether the user's ID has been verified or not.
- The *Authorisation* phase (the *post-processing* phase) that checks, in the event that the ID has been correctly verified in the previous phase, that the user with the ID has the necessary credentials to access the resource (the credentials are retrieved from a database indexed by identity).

[3] The example and the illustration below correspond to our case study concerning the experimental use of facial recognition at the entrance to two high schools in the French PACA Region. For an analysis see T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

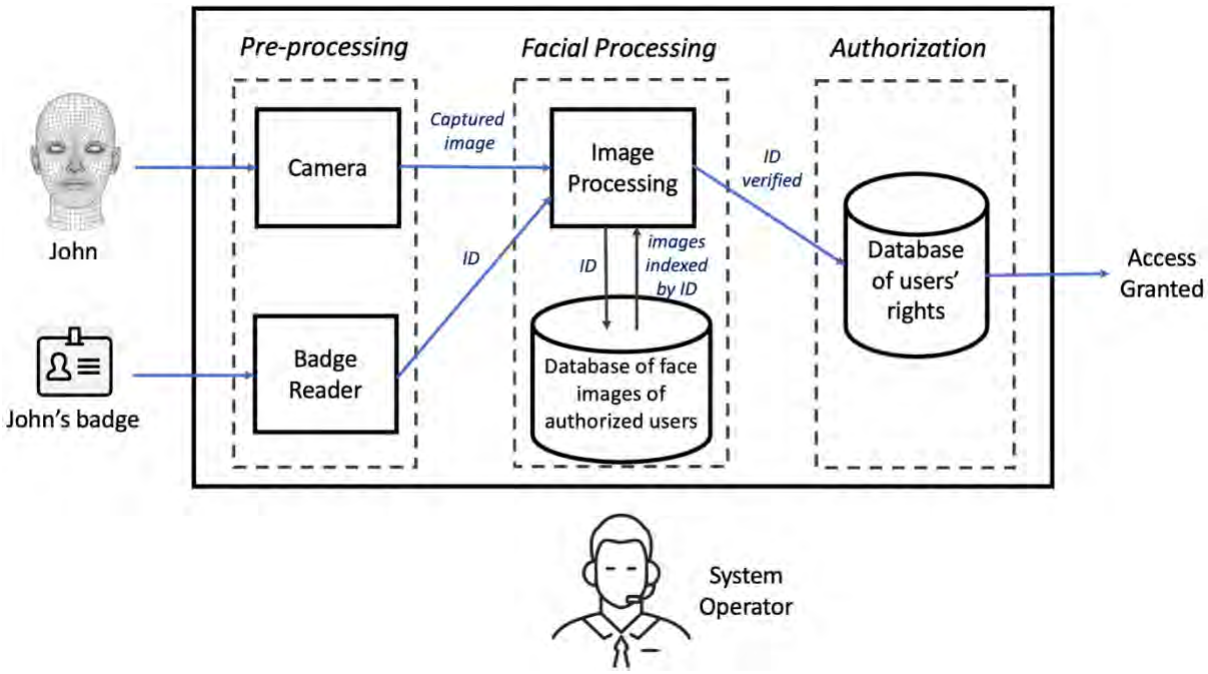


Figure 1. Example of an FR-based Authorisation Application

The risk analysis of an FR system has to consider all the components of a system, *i.e.* the facial processing component but also the pre-processing and post-processing phases (including, *inter alia*, the quality and volume of captured images, relevant human-centred processes involved, the image database, etc.). The analysis should also consider the operational component *i.e.* the risks related to the actual use of the system by the operators in the field.

From a technical point of view, the **Facial processing component (FPC)** can be characterised by:

- The FPC *inputs*
- The FPC *functionalities*
- The FPC *outputs*

1. Inputs

The inputs always include ***captured facial images ("captured faces")*** which are mostly extracted from video cameras, which may or may not be used in real time. These images may alternatively be provided, in other instances, by an operator (for instance a photo of somebody suspected for a crime is introduced into the system by a police officer). Captured facial images may concern a ***single*** person ("1"), for example a photo taken of a person at an airport e-Gate in France using the "Parafe" system, or ***all*** **of** the people ("N") present in a specific environment where biometric cameras are deployed (for instance all of the persons crossing a street in London where FR vans are deployed by the Metropolitan Police Service).

Another input can be ***reference facial images ("reference faces")***, to which the captured faces will almost always[4] be compared when face matching occurs. These **reference facial images** are often found in a ***reference database*** of faces (and may or may not be associated with identities). For instance, in all of the ways in which "Face Identification" functionality is used (see below) the *captured faces* of persons in an open or closed environment are compared to the faces in a *reference database* which, depending on the specific application, can be for instance:

- a *preexisting general database* (e.g. a general law enforcement database such as the "TAJ" in France, used for criminal investigations); or
- a *specific watchlist* (e.g. persons that have been banned from entering a stadium or a supermarket); or
- a *specific database* created for other reasons (e.g. list of passengers due to board a plane at the airport using a facial recognition application).

In our table we always refer to these databases by the symbol "M" ("Many") which denotes a *specific number* of persons present in a database. Facial images may be represented in different ways, for example as arrays of pixels or face templates[5] resulting from a face extraction and processing phase. In general reference databases contain face templates. In the following section, we use the generic term "image" when the specific choice of representation is not significant.

2. Functionalities

We distinguish **three core facial processing (FPC) functionalities**:

1) **Face verification**: Compares two faces, typically a single input captured face against a single reference face (appearing for instance in a biometric passport or in a specific index of authorised individuals). Face verification confirms that there is a match between the two faces (successful comparison). It can be used for instance to produce an authorisation outcome related to that person. Typical applications are security access protocols (such as going through automated passport control in an airport or accessing a public building) or authorisation of a purchase and link it to a bank account.

2) **Face identification**: Compares a face F with a set of faces S, for instance the captured image of an unknown person with the faces registered in the reference database.[6] It returns the image(s) from the set S, that are the closest to F.

3) **Face analysis**: Analyses the captured images of an individual in order to detect certain characteristics (gender, race, etc.) or emotional states (happiness, anger, signs that they may be lying, etc.). In contrast with the two other core functionalities, face analysis does not involve face comparison (matching).[7]

---

[4] With "Face Analysis" functionality, there is no face matching at all, and *no* reference images.
[5] A number of features characterising a face, also called a faceprint or a "biometric template".
[6] Another application can be tracking: the comparison of a single target face (the faceprint of a user) with a set of captured images (for example those obtained from a city's video surveillance system), returning all the captured images in which the target face is detected. This application can typically be used to retrieve all the images where a given suspect appears.
[7] For the relation between "face recognition" and "face analysis" see our explanations in T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe

The first two categories (face verification and face identification) involve the basic function of **face matching**, while the third category (face analysis) does not. Face matching means *"any comparison of two or more faceprints"*.[8] In **face matching**, the results can be associated with probabilities. For example, with face identification, the system can return several images each associated with a matching probability (corresponding to the similarity ratio).

- With **face verification**, face matching takes place between two images, for example a single captured image and a single reference image (1-1).[9]

- With **face identification**, face matching takes place between one image and a set of images. Faces are always verified one-by-one to all the faces in the reference database. However, in our classification table, we propose three subcategories, based on the use-cases that we have analysed, and distinguishing between a situation where there is face matching between a single captured facial image and a reference database (1-M);[10] a situation where there is face matching between captured faces of all persons present in a specific area and a reference database (N-M); and a situation where there is face matching between the captured faces of all persons present in a specific area (tracking) and the reference images of a single person (N-1) or a specific group (N-M).

- With **face analysis**, there is only one input, and there is no use of biometric templates, no face matching or identification. So, there is no "facial recognition" strictly speaking here.[11]

The above core functionalities can be applied to any number and type of image inputs, and can be assigned different purposes, giving rise to different variants, with different impacts on individual rights.

– Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

[8] See A. Schwartz, N. Sheard, B. Cyphers, "Face Recognition Technology: Commonly Used Terms", *EFF*, October 7, 2021. While we have followed in part the EFF's terminology in this paper, there are also notable differences in our proposal, including the fact that our proposal combines a distinct set of *functionalities* with the specific *applications* of each one of them.

[9] ISO defines "Face Verification" as a "biometric product function that performs a **one-to-one** comparison". Equally, the Belgian DPA considers that "the verification function consists of comparing the information presented in the second phase with the previously enrolled information belonging to a single person ("**one-to-one** comparison"). This function is particularly suitable for situations where the person wants to be authenticated and is therefore willing to voluntarily provide an identifier (such as a smart card or a badge) on the basis of which the reference biometric sample will be determined and then compared with the sample of the new collection. See Own-initiative opinion on the processing of biometric data for the authentication of persons (A/2008/017), April 9, 2008, at 5.

[10] ISO defines "Face identification" as a "biometric system function that performs a **one-to-many** search to obtain a candidate list". Equally, the Belgian DPA considers that "the identification function consists of comparing the information presented in the second phase with all the biometric information available in the biometric system and which is necessarily contained in a database ("**one-to-many** comparison"). This function will first identify the user among all the persons registered, and can then be used to authenticate the user". Own-initiative opinion on the processing of biometric data for the authentication of persons (A/2008/017), April 9, 2008, at 5.

[11] See T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term", Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

3. Outputs

The outputs of the system depend on the specific application/purpose for which it is used, the inputs received and the functionality used. Here are some examples:

- With **face verification** functionality, which is used in an application to "authorise" users (*e.g.* passport control at the border), the output will be either a "0" (failure to verify the user's ID and access denied) or a "1" (identity verified and access granted).
- With **face identification** functionality, which is used by the police in an "*individual identification"* application (*e.g.* face matching between the photo of a suspect in a criminal investigation and the images of persons in a law enforcement database) the output will be either a "0" (failure to find a match) or a list of identities associated with probabilities.

UNDERSTANDING THE *PURPOSES* OF FACIAL RECOGNITION SYSTEMS

The previous analysis defined the *technical* parameters of an FR system that are of paramount importance when classifying the uses of FR in public spaces (and, indeed, also in private spaces). However, as shown by the discussion on the "outputs", the intended purposes or "finalities" pursued by each FR system are also extremely important, not only in determining the inputs, functionalities and outputs of the system but also in assessing the risks they involve for human rights.

- Indeed, the same functionality can be used in very different ways depending on the different purposes/finalities of the system. For instance, **face identification** functionality can be used for "individual identification" purposes, such as when the police have a photo of a person who is suspected of having committed a crime and uses FR (in a 1-M way) in order to help them identify this person among the persons appearing in a law enforcement database. But the same functionality can also be used in a different application, that of "large scale face matching" (N-M), for instance by scanning the **thousands of persons** crossing a road in order to compare them with a watchlist of suspected criminals. The problems raised by the use of FR systems and the risks, as far as human rights are concerned, of the same functionality being used for different purposes and in different settings could be very different.

- Similarly, the same purpose could be served by different functionalities, raising, once again, different considerations in terms of risks and of necessity and proportionality assessments. For instance, if the purpose of the operator is to authorise access to a specific public place following access control, this could be accomplished either by using **face verification**[12] functionality (1-1, with the help of an external input such as an ID card), or by using **face identification** functionality (1-M, by storing the images of all authorised persons in a reference database).

To arrive at a satisfactory classification of the uses of FR in public spaces, it is therefore necessary, to consider both the technical elements (FPC functionalities and inputs) and the purpose for which the FR system is used (its

[12] Face "verification" is most often considered in literature as a synonym to "authentication". However, some authorities have argued that the 2 terms *are not* synonymous. The Belgian DPA, for instance, has emphasised: "We stress the fact that in the particular context of biometrics, the definition of verification has a specific meaning *that is totally distinct from the notion of authentication*. Indeed, authentication (i.e. the process of identity verification) can be achieved by both biometric functions, i.e. either by the identification function or by the verification function (see however paragraph 59 of this opinion where the Commission recommends the use of the verification function in the context of authentication)". Own-initiative opinion on the processing of biometric data for the authentication of persons (A/2008/017), April 9, 2008, at 5. To avoid confusion we mostly use in these reports the term "verification". For a detailed analysis see T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

"applications") that will determine the outputs of the system and will greatly influence the risk assessment. The conditions of operation of the system are also of prime importance in this respect (operators using it, authorisations, accountability measures, etc.).

UNDERSTANDING THE CLASSIFICATION TABLE

Based on all the previous considerations we are able to present a detailed classification of the uses of FR in public spaces.

The table is based on the core functionalities identified in the previous section. More precisely, we consider successively applications based on face verification (Section 1), face search/identification (Section 2), face clustering (Section 3) and face analysis (Section 4).

For each functionality the table presents, from left to right:

- The specific "**Application**" of the FR system, in other words the general purpose pursued by its operator.

- The basic features ("1", "N" or "M") of the inputs of the system, namely the **"Captured Faces" (*i.e.* captured facial images)** on the one hand and the **"Reference Faces" (reference facial images)** on the other hand. As explained earlier:

  - **"1"** refers to a *single* face introduced as an input to the system, for instance the photo of a person taken at an eGate while passing through border control at the airport (example of "1" in "Captured Faces"); or the photo of this same person appearing in his or her biometric passport (example of "1" in "Reference Faces").

  - **"N"** refers to the faces of *all* persons present in a specific public space (for instance a station or a road) which are captured as an input by an FR system before processing them to check, for instance, if they match the faces in a database.

  - **"M"** refers to the faces of a *specific and pre-determined number of persons appearing in a reference database*. Depending on the situation, "M" could refer to just a few persons (for instance Air France passengers boarding an airplane who are listed in the database of a FRT application such as "MONA" in France); hundreds of persons (for instance 1200 persons in a watchlist); or even to millions of persons (for instance those who appear in a general law enforcement database such as the TAJ in France).

- An **"Explanation"** of the functionality used along with the specific application.

- **"Examples"** of "selected cases" for each category that we have studied in detail during our "mapping" of the use of FR in public spaces in Europe.[13] Several other cases have been studied and will be presented in our report, but it was

[13] A detailed presentation of these case studies will be published at the end of this project. See T. Christakis, et al, "Mapping the Use of Facial Recognition in Public Spaces in Europe – 25 Selected Case Studies", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, forthcoming.

impossible to show all these "examples" in our table. Also please note again that only uses of FR *in public spaces* are considered in this study.[14]

We should emphasise that the tables below are not meant to be comprehensive, neither in terms of categories of existing techniques and applications, nor in terms of relevant criteria.

In terms of existing techniques and applications, it should be noted that the biometric industry is developing a great variety of tools for very different applications.[15] Our table does not intend to be exhaustive. It intends instead to present in an accessible way the main FR functionalities and applications that have been used until now in public spaces in Europe. It should also be noted that in some cases, depending on how the purposes pursued by an operator are managed, a **combination** of these techniques and applications can be used.

In terms of relevant criteria, the timing criterion (real time versus post-processing), which is central in the draft EU AI Regulation[16] does not appear in the table. This does not mean that it should not be taken into consideration, for instance, in a Data Protection Impact Assessment, but we believe that criteria such as scale ("individual" versus "large scale") are often more significant. It should also be noted that the relevance of this timing criterion has been challenged by NGOs[17] and scholars,[18] as we will discuss in Parts 4 and 5 of the MAPFRE Reports.

The main objective of the tables below is thus to provide a useful tool for disaggregating the different forms and applications of FRT. This, in turn, should allow, we hope, for the debate and regulation on facial recognition to be focused more accurately.

---

[14] Our study does not cover, for instance, a case such as the use of FR by Polish authorities to ensure that a person respects the quarantine rules and isolates at home due to Covid-19. For our definition of public spaces see T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term", Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

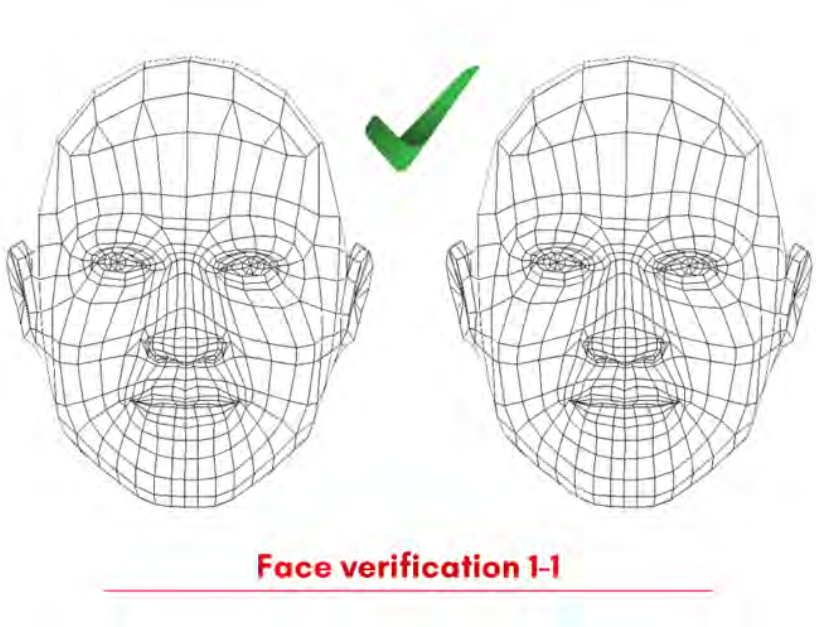
[15] See for instance the impressive number of tools developed by the 130 facial recognition start-ups listed in our study Becuywe, M., Beliaeva, T., Beltran Gautron, S., Christakis T., El Bouchikhi, M., Guerraz, A. "Landscape of start-ups developing facial recognition. Analysis and legal considerations", AI-Regulation.com, Skopai.com, January 2022.

[16] Article 3(37) of the draft AI Regulation defines "real-time remote biometric identification system" as "system whereby the capturing of biometric data, the comparison and the identification all occur **without a significant delay**. This comprises not only instant identification, but also **limited short delays** in order to avoid circumvention". Article 3(38) of the same draft defines **"post remote biometric identification"** negatively as "a remote biometric identification system other than a 'real-time' remote biometric identification system". Emphasis added.

[17] NGOs (such as those behind the reclaim your face campaign) challenge the relevance of this criterion and ask "to ensure that all uses of remote biometric identification (whether real-time or post) in publicly-accessible spaces are included in the prohibition" of the draft EU AI Regulation. See for instance here.

[18] See for instance N. Ni Loidenain, "A Trustworthy Framework that Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics", *Information Law and Policy Centre*, Aug 4, 2021, arguing that "considerable legal uncertainty surrounds the key categories of 'real-time' and 'post' remote biometric identification systems", that the draft AI Act "is silent on the crucial question of what 'a significant delay' actually entails" and ultimately asking: "why does the 'significant delay' between the original collection of a photo/image of an individual and its processing by law enforcement for facial recognition/emotion recognition purposes determine its intrusiveness?".

1. FACE VERIFICATION



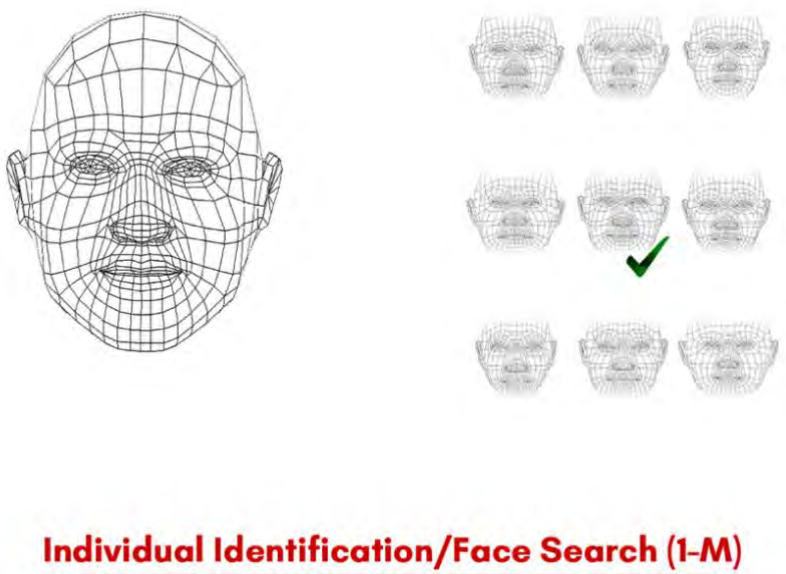
Application	Captured Faces	Reference Faces	Explanation	Examples
Authorisation using a biometric token	1	1	Compares a single face against a reference image stored in a biometric token of the user (*e.g.* a passport). Face recognition is used to confirm that there is indeed a match between the two images. This may be used in security access control protocols.	PARAFE Automated Passport control at the border (FR)
Authorisation using an ID token	1	1(in M)	Compares a single face against a single reference indexed in a database. A token stores an identifier of the user. The token can be in the form of a badge, QR code in a smartphone, etc. It is provided as an input by a person and links to his/her specific image stored in this database "1(in M)". Face recognition is used to confirm that there is indeed a match between the two images. This may be used for instance in access controls in a closed space (*e.g* a school).	PACA Schools Access Control in High schools in the South of France

2. FACE IDENTIFICATION

As mentioned earlier, with face identification, face matching takes place between one image and a set of images. Technically speaking, captured faces are always verified one-by-one to all the faces in the reference database. However, based on the use-cases that we have analysed and the *purposes* of the FR systems, we think that it is useful to distinguish three subcategories of face identification applications: applications that only use 1 captured facial image (Section 2.1); applications that capture faces of all of the people in a specific venue (Section 2.2); and tracking applications that focus on a single reference face but which capture everyone in a specific venue (Section 2.3). These distinctions result from our analysis of different use-cases and the fact that these three subcategories (and their specific applications) could raise distinct problems and have different impacts on fundamental rights. For instance, the risks raised by "large scale face matching" are of a different nature than the risks raised by an application of an individual identification, as we will explain in subsequent reports.

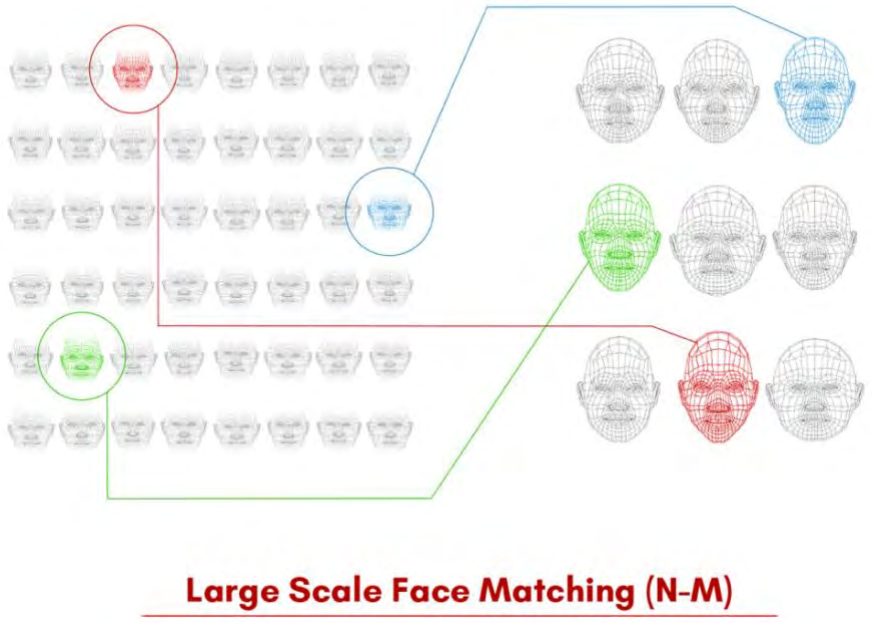
2.1 Individual Identification/Face Search (1-M)

This subcategory is characterized by the fact that the search is based on a single captured facial image. This can be either an existing photo of an unknown person (captured, for instance, by a webcam, a surveillance camera or found on the internet) or an image captured at an eGate or by a specific device present at a checkpoint (for instance at the entrance to a venue).



Application	Captured Faces	Reference Faces	Explanation	Examples
Individual Identification	1	M	Tries to identify a person for which a face picture is available and relies on a database of face images associated with identities. Mostly used for public security purposes (*e.g.* by the police to identify suspects in criminal investigations).	TAJ (FR) SARI Enterprise (IT) South Wales Police (UK) Clearview Olympic Stadium (IT) (…)
Authorisation without using a token	1	M	Authorises a user by searching if his faceprint appears in a database of authorised users.	Molenbeek Stadium (BE) MONA (FR) AENA (ES) Payments in School Canteens (UK) (…)

2.2 Large Scale[19] Face Matching (N-M)



Application	Captured Faces	Reference Faces	Explanation	Examples
Surveillance of an Open or Restricted Public Place[20]	N	M (or 1)	Monitors a public place (the entrance to a stadium, a crowd attending a specific event, the streets of a city, etc.) to identify people in a database (*e.g.* used by the police or private security firms to identify people in a watchlist). Can also be used to search for a missing child in a public place (in this case M=1).	South Wales Police (UK) London MPS (UK) Mercadona Supermarkets (ES) Brondby IF (DK) Zaventem Airport (BE) SARI Real Time (IT) (…)

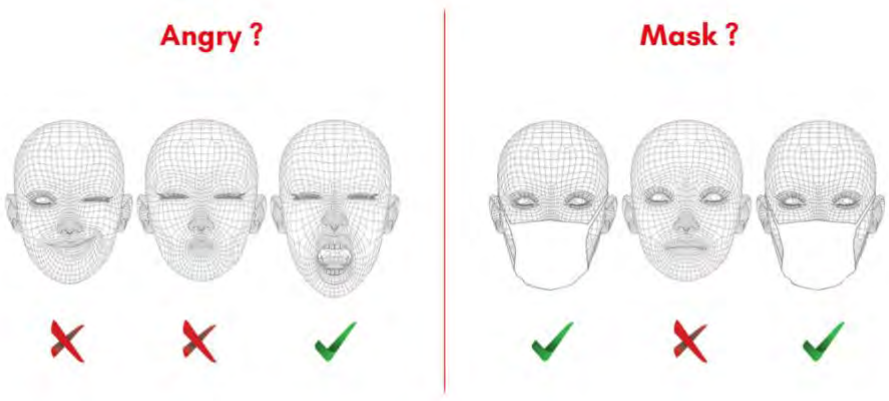
[19] By "large scale" we mean that the captured images systematically contain the images of all the people present in an open or closed environment and creates biometric templates of these people in order to compare them with a watchlist. The fact that the system may often immediately erase the templates of people who do not "match" changes nothing in terms of the "large scale" character of the functionality.
[20] For the definitions of an "Open" public space and a "Restricted" public space see T. Christakis, et al., "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

2.3 Targeted Face Tracking (N-1)

Application	Captured Faces	Reference Faces	Explanation	Examples
Targeted Face Tracking	N	1 (or M)	Tracks an individual (or several individuals) using video cameras in a geographic zone (for example to track where a suspect is moving in a city).	Trial proposed during Nice Carnival (FR) or phase 2 in Berlin Station (DE)

3. FACE ANALYSIS

In contrast to the two other core functionalities, face analysis does not involve face comparison (matching). Therefore, it does not require reference images and it does not strictly speaking represent one of the "face recognition" techniques, despite the use of facial processing.



Face Analysis

Application	Captured Faces	Reference Faces	Explanation	Examples
Categorisation, Emotion Recognition	1 or N		Tries to infer specific attributes from faces (e.g. emotions, signs that the person may be lying, gender, their estimated age, whether a person is wearing a mask at a train station, etc.).	iBorderCtrl project (HU, GR and LV) Datakalab (FR)

HOW TO CITE THIS REPORT:

T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022

The Chair on the Legal and Regulatory Implications of Artificial Intelligence

The Chair on the Legal and Regulatory Implications of Artificial Intelligence is part of the Multidisiplinary Institute in Artificial Intelligence (MIAI) established at Grenoble Alpes University in France. Its objective is to analyse the legal and regulatory questions raised by artificial intelligence and to contribute to the national, European and international debates on these issues.

The Chair has been built upon the highly successful interdisciplinary network created within the Grenoble Alpes Data and CyberSecurity Institutes. Its members are experts in law, economics, security, computer and data science, all actively working in the fields of data protection, privacy, cybersecurity and AI. They collaborate actively with and provide expert advice to major national, European and international institutions.

The Chair's work can be found on its website: AI-Regulation.Com.

THANKS TO THE FOLLOWING INSTITUTIONS FOR THEIR SUPPORT:

FUTURE OF PRIVACY FORUM

AI-REGULATION.COM

MIAI Grenoble Alpes

Inria inventors for the digital world

UGA Université Grenoble Alpes

CESICE Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes