MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE A QUEST FOR CLARITY: UNPICKING THE ”CATCH-ALL” TERM

Theodore Christakis, Karine Bannelier-Christakis, Claude Castelluccia, Daniel Le Métayer

MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE

MAY 2022

PART 1

A QUEST FOR CLARITY: UNPICKING THE "CATCH-ALL" TERM

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

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.

MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE
MAY 2022
PART 1
A QUEST FOR CLARITY: UNPICKING THE "CATCH-ALL" TERM

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Regulating the use of facial recognition and face analysis in public spaces is undoubtedly one of the most pressing issues today when it comes to the regulation of artificial intelligence in democratic societies. There is an important debate going on worldwide about the "red lines" that should be established by regulators in order to prevent people's freedoms being endangered as the result of the use of facial recognition technologies (FRT). In Europe especially, where privacy, data protection and human rights lie at the very heart of the European integration project, this debate is more necessary and pressing than ever. The importance of this issue is reflected in the ongoing legislative work that has followed the European Commission's introduction, in April 2021, of the draft AI regulation, which includes several important proposals to regulate the use of facial recognition.

Curiously, though, the debate about these fundamental questions is taking place in the absence of a profound assessment of how *existing* European law is being applied to these issues. Furthermore, the debate on these issues in Europe is also characterised by a high level of imprecision. Journalists, activists and politicians sometimes have a tendency to treat "facial recognition" as a single monolithic bloc, **lumping the different functionalities and uses of facial recognition together**. In contrast, in an important Opinion published in 2019 the French DPA, CNIL, stressed the importance of clarity and precision to fostering the conditions necessary for an informed and useful debate. "**Behind the catch-all term, there are multiple use cases"** said the CNIL, adding that "**in this context, a use-by-use approach must be applied".**

This is precisely the main objective of the "**MAP**ping the use of **F**acial **R**ecognition in public spaces in **E**urope" (MAPFRE) project. Our intention is to offer a detailed independent study that separately presents and analyses the different categories of FRT use in publicly accessible places in the European Union and the UK. The intention of our project is to publish a series of reports which include:

- the general context and objectives of the project as well as an analysis of the problem of definitions (Part 1);
- a detailed explanation of the different facial processing functionalities and applications in public spaces in Europe using a classification table, illustrations and charts (Part 2);
- a first ever detailed report on the use of facial recognition for authorisation purposes in public spaces in Europe (Part 3);
- a report which focuses on the important issue of the use of FRT in criminal investigations (Part 4);
- a deep dive into the equally important issue of large-scale face matching/identification (what the AI draft regulation calls "real-time remote biometric identification") (Part 5);
- and, finally, a report which discusses the use of "face analysis" in public spaces (which remains marginal in Europe but is likely to develop in the future) and which also presents the general perspectives and recommendations of the MAPFRE project (Part 6).

At the end of this project, we will also present an analysis of "25 selected cases", illustrating the different categories in our classification table, as well as analysing other cases more briefly.

The current "Report 1" presents the major positions on the debate surrounding the use of FRT as well as the preliminary positions adopted by Members of the European Council and Parliament during the ongoing legislative process concerning the draft AI regulation.

It then dives into the important issue of **definitions**. Our study shows that the existing definition of "biometric data" in the GDPR and the LED is problematic and confusing. This has compelled some actors to propose amending it in the draft AI Act. However, the consequences of such an amendment could be significant as it is difficult to imagine how we could have a different definition of "biometric data" in the GDPR and the LED to that in the AI Act. Other stakeholders, especially the Rapporteurs of the European Parliament, have instead proposed creating an entirely new category called "biometrics-based data". While the intentions of the Rapporteurs are understandable, the creation of a new category so similar to the original one might create further confusion in this field.

Following this important discussion, we explain the **scope** of our study. We cover the use of both "**facial recognition"** and **"face analysis"** in public spaces (and we explain the difference between the two terms). Drawing on the draft EU AI Regulation, we also define how we use the term "public spaces". Finally, with regard to the *territorial scope* of our study, we explain why we have decided to include cases that originate not only from EU Member States but also from the UK.

Finally, we explain the **methodological tools** that we have used. The first tool that we have elaborated is a **"Classification Table"**, which illustrates the uses of facial recognition/analysis in public spaces. This table, to be published in "Part 2" of our MAPFRE series, tries to present in the most accurate and accessible way the different facial processing functionalities and applications used in public spaces. The second methodological tool that we have elaborated is a **detailed analytical framework** which asks a number of key questions. The template for this analytical framework is presented in an annex to this paper. To summarise it, it involves 3 series of questions: a series of questions on the facts and technical details of the use case; a second series of questions on Human Rights and the principles relating to the processing of personal data; and a third part which tries to identify whether any additional guarantees were offered by the data controller, focusing on issues such as accountability and transparency, whether a Data Protection Impact Assessment (DPIA) was conducted, and whether there was an evaluation of the effectiveness of the system. We have applied this analytical framework as a means of analysing 25 interesting use cases in detail, covering the various functionalities and applications found in our classification table. Aside from these 25 "selected" case studies, which we will publish at the end of the project, we have extensively analysed several other important cases of FRT deployment in public spaces in Europe.

We hope that our study will be useful not only to policy-makers, stakeholders, scholars and citizens who may be interested in the issue of facial recognition/analysis, but also anyone interested in how major human rights and data protection principles, such as the principle of lawfulness, the principles of necessity and proportionality or other principles relating to the processing of personal data, are interpreted. Indeed, during our research into how facial recognition systems are deployed in Europe, we found a treasure trove of information that includes documents produced by data controllers, legal challenges introduced by civil society, positions of DPAs, judgments of national courts, articles published by scholars and journalists, and other material. We expect that all of this material will be of great interest not only in terms of the regulation of facial recognition, but also in terms of understanding how the GDPR, the LED and European HR Law apply to a number of important fields.

Mapping the Use of Facial Recognition
in Public Spaces in Europe

Part 1
A QUEST FOR CLARITY: UNPICKING THE "CATCH-ALL" TERM

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

I. THE NEED FOR MEANINGFUL DEBATE ON FACIAL RECOGNITION

Regulating the use of facial recognition and face analysis in public spaces is undoubtedly the most pressing issue today when it comes to the regulation of artificial intelligence in democratic societies. The impressive progress that has been made in recent years in the field of image processing, particularly where facial recognition is concerned, incentivises the increased use of these new technologies by private and public actors. But at the same time, these developments involve serious risks to human rights; raise ethical questions and the spectre of power imbalances and biases; arouse concern about lack of transparency and accountability; and foster the fear of function creep and the slippery slope towards a surveillance society. There is an important debate going on worldwide about the "red lines" that should be established by regulators in order to prevent endangering people's freedoms as the result of the use of facial recognition technologies. This debate is crucial. Indeed, beyond the technicalities of the debate, political choices have to be made in order to shape what our society will look like tomorrow: given the power of this technology, how can we reconcile the protection of fundamental rights and freedoms with security, economic considerations and technological competitiveness issues?

In Europe especially, where privacy, data protection and human rights lie at the very heart of the European integration project, this debate is more necessary and pressing than ever. This importance is reflected in the ongoing legislative work that has followed the European Commission's April 2021 introduction of the draft AI regulation,[1] which includes several important proposals to regulate the use of facial recognition, proposals analysed in detail in our previous AI-Regulation Chair publications.[2] Indeed, one could say that the provisions of the draft AI Act on the use of "remote biometric identification systems" [3] in publicly accessible spaces, a category both narrower and broader to "facial recognition",[4] are those that are generating among the biggest reactions among various stakeholders,[5] together with issues such as regulation of high risk systems and

[1] Artificial Intelligence Act, European Commission, April 21, 2021.

[2] See: T. Christakis, M. Becuywe, "Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation", *European Law Blog*, May 4, 2021 and T. Christakis, Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021., *AI.Regulation.Com*, May 27, 2021. See also Facial Recognition in the Draft AI Regulation: Useful Materials, *AI.Regulation.Com*, May 4, 2021.

[3] The Commission's proposals only focus on *"remote biometric identification (RBI) systems"* defined in Article 3(36) of the draft AI Act as "AI system(s) for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified". More specifically, the Commission's draft aims to prohibit the use of "real-time remote biometric identification systems" by law enforcement authorities – while introducing a series of exceptions. The Commission's proposals do not concern, nonetheless, the use of "remote biometric identification systems" by private or public actors for purposes other than law enforcement.

[4] See infra, Part IV.

[5] For a few among these reactions see *infra* Part III.

transparency obligations.

Curiously, though, the debate about these fundamental questions is taking place **in the absence of a profound assessment of how *existing* European law has been applied to these issues**. Contrary to other countries, such as the United States, where regulatory initiatives in the field of facial recognition are often created without preexisting general data protection rules, in Europe an important corpus of rules (which are mainly found in the GDPR[6] and the Law Enforcement Directive[7]) already exists on the processing of *biometric data* as well as the processing of *biometrics-based personal data* – terms and distinctions that we will explain later in this report. And this is occurring despite the fact that we have, as of today, an important number of use cases involving the actual or intended deployment of facial recognition in public spaces in Europe, marked by a raft of legal and technical documents produced by data controllers, opinions published by Data Protection Authorities (DPAs) and decisions rendered by Courts. What could practice and case law teach us about the strengths and weaknesses of existing rules in order to better design any future legislative intervention?

Furthermore, **the debate on these issues in Europe is also characterised by a high level of imprecision**. Journalists, activists and politicians sometimes have a tendency to treat "facial recognition" as a single monolithic bloc, **lumping the different functionalities and uses of facial recognition together**.[8] In contrast, in an important Opinion published in 2019 the French DPA, "*Commission National de l'Informatique et des Libertés*" (CNIL), stressed the importance of clarity, precision and a use-by-use approach to fostering the conditions necessary for an informed and useful debate on the fundamental issue of facial recognition.

CNIL: "Behind the catch-all term..." The need for a use-by-use approach in order to ensure that an informed debate takes place

In response to a number of developments in France concerning the use of facial recognition, ranging from calls from private companies and French politicians to the use or "experimental use" of facial recognition technologies, to calls for a "moratorium" or a "ban" on such use, the French DPA published a very important opinion in November 2019 entitled: "Facial Recognition: For a Debate Living up to the Challenges".

In this opinion, the CNIL starts by stating:

*"Facial recognition is raising new questions about societal choices and, as such, interest in the subject is growing on national, European and global public agendas alike. […] [T]he **CNIL called for a democratic debate to be held on the new uses of video cameras, with a particular focus on facial recognition technologies.** Amid an increase in their use and the public authorities' growing awareness of the opportunities and risks they pose, this technology has risen to the top of the public*

[6] The General Data Protection Regulation (GDPR) is an EU regulation which applies automatically on the territory of all Member States and which aims at providing a legal framework for data processing when personal data is collected and processed by entities other than law enforcement authorities.

[7] The Law Enforcement Directive is an EU legislation which provides a legal framework for personal data processing by law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. However, a domestic law must incorporate this directive into each Member State's internal legal order.

[8] There is also a tendency to frame debates over surveillance in very binary utopian v dystopian terms which further depletes the quality of the debate. See for instance P. Fussey, A. Sandhu, A., "Surveillance Arbitration in the Era of Digital Policing", *Theoretical Criminology*, vol. 26(1), (2021), pp. 3–22.

agenda. ***This debate is crucial”.***

However, the CNIL stresses that there are some important methodological difficulties to be overcome in order to conduct this debate in a meaningful way. It notes:

*“****This proactive and forward-looking debate must meaningfully address the issues at stake.*** *[…] To ensure an informed debate,* ***the terms of the debate must themselves be clear, with an understanding of what facial recognition means.*** *This will avoid confusion between different uses of this technology where the issues raised are not the same, or with related technologies of a different nature.* *[…]*

The current debate is sometimes distorted by a poor grasp of this technology and of how it exactly works. This can lead to the risks being inadequately described and to confusions between facial recognition and related technologies which also use images at the core of their processing. Another problem arises due to "facial recognition" being referred to in the singular, when it is actually used in many different ways – and the issues involved may vary accordingly, for example in terms of the control people have over their data. By extrapolating from well-established cases of use, there is a high risk of jumping to conclusions about this technology”.

Taking into consideration these methodological difficulties, the CNIL emphasises in its opinion that “**Behind the catch-all term, there are multiple use cases”** and that “**in this context, a use-by-use approach must be applied”.**[9]

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

II. OBJECTIVES OF THE MAPFRE PROJECT

In line with the CNIL's reasoning in its 2019 Opinion, the authors of this study argue that for such debates on facial recognition to be productive and accurate, it is essential to ensure that we apply a common and robust intellectual framework and that arguments be expressed and confronted in a rigorous way. In particular, it is critical that we avoid, as much as possible, using preconceptions, and that we distinguish established facts from assumptions or opinions, and treat different use cases, which may raise different issues and risks, distinctly.

It is precisely this that is the main objective of the "**MAP**ping the use of **F**acial **R**ecognition in public spaces in **E**urope" (MAPFRE) project. It is the intention of our project to put together for the first time,[10] a detailed independent report that *separately* presents and analyses the different categories of FRT use cases (past, ongoing or projected) in publicly accessible places in the European Union and the UK and identifies the current trends. To be more precise, our project intends to:

- ➢ Propose a classification and "mapping" method for the different categories of use of facial recognition and face analysis applications in publicly accessible spaces in the EU as well as the UK.
- ➢ Publish a series of reports to this end, focusing on:
  - the general context and objectives of the project (Part 1);
  - a detailed explanation of the different facial processing functionalities and applications in public spaces in Europe (EU Member States and the UK) using a classification table and illustrations (Part 2);

[10] Despite high interest in the use and regulation of facial recognition in Europe, few extensive studies on the topic exist and none undertake a use-by-use analysis as our current study intends to do. The most extensive report on the issue of facial recognition in Europe was published in French under the direction of Caroline Lequesne Roth and a team of researchers who did a remarkable job of providing basic information about certain uses of facial recognition in Europe as well as the more general European legal framework (see also this). However, this study applies the general label of "facial recognition" to all of these cases and does not analyse the distinct legal, technical and other characteristics of FR, including the potential risks to human rights, of the different categories of uses of facial recognition. Other studies have recently been initiated by stakeholders, who are campaigning for a ban on facial recognition in public spaces in Europe and are focusing on "biometric mass surveillance". Taking into consideration the subject matter of these studies, they logically conflate analysis of cases that concern the use (or projected use) of facial recognition in public spaces with several other cases which are not related to the use of facial recognition or face analysis in public spaces. EdRi's 2020 report, for instance, on "The Rise and Rise of Biometric Mass Surveillance in the EU", includes case studies on the use of fingerprints in biometric IDs, the "living labs" experiment, the Pegasus spyware, video surveillance in public spaces and facial recognition uses in private spaces to control quarantining at home due to Covid-19. The first of two recent reports on "biometric and behavioural mass surveillance", commissioned by the Greens and published in October 2021, similarly includes case studies that are not related to the use of facial recognition or face processing in public spaces, such as projects concerning detection of suspicious behaviour (where the system does not record any characteristics specific to an individual) or the use of apps for quarantining at home. As for the second report on "biometric and behavioural mass surveillance", also commissioned by the Greens and published in February 2022, it goes even further by including in its "case studies" an analysis of issues such as E-administration, public usage of surveillance technologies by intelligence services, video-surveillance in general, or the issuance of identity documents (including biometric passports) by countries as diverse as France and Romania.

  - a first ever detailed report on the use of facial recognition for authorisation purposes in public spaces in Europe (Part 3);
  - a report which focuses on the important issue of the use of facial recognition and individual identification in criminal investigations (Part 4);
  - a deep dive into the equally important issue of large-scale face matching/identification (Part 5);
  - and, finally, a report which discusses the use of "face analysis" in public spaces (which remains marginal in Europe but is likely to develop in the future) and which provides the general perspectives and recommendations of the MAPFRE project (Part 6).

- Present an analysis of "25 selected cases", illustrating the different categories of our classification table, as well as analysing other cases more briefly.
- Offer a deep insight into the legal framework (EU Law, national laws) under which FRT is being used in various ways in public spaces in Europe, and the management policies and protocols gradually being put in place.
- Assess to what extent the various use cases have applied basic ethical and legal principles, including the principles of transparency, accountability, necessity, proportionality and control as well as the other principles relating to processing of personal data: purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality.
- Present a detailed comparison of the positions of Data Protection Authorities and European Courts on the various uses of FRT and identify points of convergence but also points of divergence.
- Discuss the technical choices which impact on the risks posed by facial recognition, try to identify whether Data Protection Impact Assessments (DPIA) and evaluations of the effectiveness of the solutions on the ground have been carried out, and determine whether these are based on solid methodology.
- Assess the strengths and weaknesses of or potential gaps in the current European legal framework.
- Present options and make recommendations that may be useful for future regulation and analysis of face recognition in Europe.

We hope that our reports, which are the product of several months of work by a multidisciplinary team of AI.Regulation Chair researchers, will be helpful to all of the stakeholders in this important European debate: policy makers; civil society; companies that intend to develop or market FRT products and solutions; data controllers; DPAs; lawyers who may be working on these issues. It is also of prime importance that European citizens, despite the complexity of these issues,[11] can find valuable and independent information about these matters, presented in the most accessible way possible, in order to be able to take part in this debate in an informed way.

[11] The UK's Ada Lovelace Institute found that most people do not know enough about facial recognition technology to have an informed opinion on its use, see "Beyond face value: public attitudes to facial recognition technology", Report, *Ada Lovelace Institute*, September 2019, at 4-5.

III. UNDERSTANDING THE POLITICAL LANDSCAPE

Before diving into the problem of definitions and explaining the exact scope of our study and the methodological tools that we have used, it is worth quickly reviewing the major positions on the debate surrounding the use of FRT. We will start by looking at those positions that support the use of FRT in public spaces while often calling for regulation, safeguards and “red lines” (1). We will then move on to those that call for a ban on such use, or a ban on “biometric mass surveillance” (2). And we will end by briefly considering the preliminary positions adopted by Members of the European Council and Parliament during the ongoing legislative process concerning the draft AI regulation (3).

1. Voices in Favor of the Use or “Testing” of FRT in Public Spaces

Several stakeholders have called for the “responsible” use of FRT in public spaces, and have stressed that this technology, if adequately regulated, could accomplish important legitimate aims (including security) and bring considerable societal benefit.

These stakeholders range from technology providers which cite, among other things, the importance of being able to work on developing these important technologies whilst not entirely and permanently ceding the FRT market to companies from the United States, Israel, China or Russia; other private actors who consider that the use of FRT may offer enormous benefits to their business model, and improve customer service and the customer experience; and security, law enforcement and other public authorities (such as those that promote “smart cities”) who stress that FRT has “a lot to offer as a tool for enhancing public security” provided that they are used responsibly and ethically.[12] And politicians who take into consideration all of these and other arguments in order to plead in favor of the use of FRT in public spaces provided that all of the necessary controls and safeguards are put in place. The attitude of several members of parliament of the ruling party in France (affiliated to the Renew political group in the European Parliament) is very telling in this respect.

France: “Experimenting” with facial recognition

In France a number of members of the government, or MPs of the ruling party, have called, over the last few years, for the development of facial recognition by means of an experimental approach using pilot projects.[13]

[12] See for instance this article by the Deputy chairman of the CDU/CSU parliamentary group responsible for the areas of legal affairs T. Frei, “Facial recognition can make us safer”, *about:intel European Voices on Surveillance*, November 10, 2020.

[13] Similar calls for “experimental approaches” with FRT are made by politicians in several other countries. They are often met with skepticism by civil society organisations who consider that “trials” are more about optimising use and convincing the public than about experimenting in any meaningful or scientific sense.

For instance, Cédric O, French Secretary of State for Digital Transition and Electronic Communications, stated that:

"First of all, experiments are needed, because the technology is evolving rapidly, but identification does not yet work perfectly and the security of authentication is not fully guaranteed at this stage either. We therefore need more experiments, under the supervision of Parliament and civil society. Then we will have a parliamentary debate on our collective choices".[14]

Didier Baichère, an MP from the ruling party well known for his work on FRT, introduced a draft law bill in May 2021, which was backed by other MPs from the same party, and allows for facial recognition in public spaces to be piloted for certain specific purposes, including law enforcement. The bill (not yet discussed or adopted) reads as follows:

"This bill aims to allow scientific experimentation with four specific use cases for facial recognition, while leaving open the possibility of categorising others if the civil society/research oversight committee deems it necessary:

1) Facial recognition access (flow management): Flow management would be aided by a facial recognition system that would replace ticketing for access to premises, events or public transport. Facial recognition access also allows payment, [...].

2) Safety and security in spaces: These situations include law enforcement and public safety activities such as customs, searching for missing persons or tracking a suspect.

3) Marketing and customer services (solicited or unsolicited offers): This use case refers to all marketing, advertising and customer services based on facial recognition (e.g. personalised shopping, emotion recognition).

4) Health or social services: This use case would allow the use of facial recognition to authenticate patients, identify or track medical conditions, or assist people such as wearable devices for the blind that identify people".[15]

This draft bill also aimed to introduce procedural and substantive safeguards for these pilot projects.

Similarly, French MP Jean-Michel MIS delivered a report in September 2021 commissioned by the French Prime Minister entitled "For a responsible and socially acceptable use of security technologies", in which he talks about the alleged efficiency of FRT where security is concerned, and also suggests deploying pilot projects. The Rapporteur acknowledges the criticism expressed by NGOs and other human rights specialists about the risks that the use of facial recognition and other surveillance technology may pose for human rights, but he refuses to reject the use of biometrics, as a matter of principle, using the following argument:

In its November 2019 Opinion on FRT, the French DPA, CNIL, insisted that such trials must adopt a "genuinely experimental approach" and "a rigorous experimental methodology". The CNIL also insisted that "experimentations should not have the ethical purpose or effect of accustoming people to intrusive surveillance techniques, with the more or less explicit aim of preparing the ground for further deployment". See CNIL, "Facial Recognition: For a debate living up to the challenges", November 2019.

[14] Mission d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles - Audition de M. Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques, 16 Mars 2022, available at: Commission des lois : compte rendu de la semaine du 14 mars 2022 (senat.fr). Our translation.

[15] PROPOSITION DE LOI d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle, available at: Proposition de loi nº 4127 d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle (assemblee-nationale.fr)

"[i]t is imperative that these concerns be addressed because they encompass an aspiration that is synonymous with modern democracies, which concerns public freedoms and individual freedoms (covering the right to privacy and anonymity in public spaces). But these rights cannot be sufficient in themselves, in absolute terms. The assessment of the public interest and the function of the state involves balancing them with other proportionate objectives, such as the shared security of individuals and the community".

The Rapporteur recommends initiating: *"in the short term a programme of targeted experiments using real-time facial recognition in public spaces, under constant law, in partnership with major local authorities and operators, based on the model of the Nice Carnival experiment conducted in 2019".*

He also recommends that care is taken to: *"consider a legislative change to open up a framework that will enable real-life employment of the FRT for a limited period. A draft or proposed law would allow for a parliamentary debate on real-time facial recognition in public spaces. This experimentation should be limited for the time being to the fight against terrorism".* [16]

It is interesting to note, nonetheless, that despite the aforementioned strong support of the majority, these recommendations have not yet been observed, and the draft bill on the experimental approach has not been adopted.[17] In terms of what may have led the majority not to push for such pilot projects or legislative reforms before the 2022 presidential and legislative elections, it is more likely due to the fact that facial recognition is considered a controversial issue from a political point of view, than the advent of the Covid-19 pandemic.[18] The result of this, as we will see in our subsequent use-by-use analysis, is that all of the pilot projects involving the use of FRT in public spaces in France have been based on consent and the GDPR – and have often been stopped by the French DPA. This has sometimes provoked strong political reaction, especially where the following "landmark" case is concerned.

When two French politicians launched an attack on the French DPA for its positions on facial recognition

In December 2018 the Provence-Alpes-Côte d'Azur Region (PACA) in the south of France decided to experiment with facial recognition at the entrances of two High Schools. The systems were put in place in February 2019 in order to "assist the personnel of the high schools" in only permitting access to

[16] MIS (J-M.), "Pour un usage responsable et acceptable par la société des technologies de sécurité", Volume I, Rapport, Septembre 2021.

[17] While our study was under press, the French Senate adopted "unanimously" a report which recommends, similar to the previously mentioned proposals, the **adoption of a law** providing an "adequate legal framework" for the implementation of various FRT experiments over a **period of three years**. One of the Rapporteurs explained that: "it is necessary to accept that we can experiment with a certain number of cases of use which may be linked to terrorism, the protection of major sports sites, or the need for the police to check that the person in front of them is not registered in the criminal database. All this can be done, but in a controlled and proportionate manner". The Rapporteur also explained that "in the long term, the results of the experiments could lead to a more detailed legislative process". He indicated that "the bill on FRT experimentation could be submitted to Parliament in the autumn". Public Senat, "Reconnaissance Faciale : le Sénat plaide pour une loi d'expérimentation", May 10, 2022. Our translation. See also the press release of the French Senate.

[18] See for instance the declaration of French Secretary of State for Digital Affairs Cédric O, announcing that, contrary to initials projects there should finally be no use of FRT during the 2024 Paris Olympic Games: "Could we have had a calm debate on the deployment of facial recognition in the Olympic Games while we have a presidential election… I am not sure. I'm even sure of the opposite". Cited in *ibid*.

authorised students, and preventing identity card theft or misuse. As we will see in Part 3 of our study (dedicated to the issue of "Facial Recognition for Authorisation Purposes") the French DPA, CNIL, stopped these pilot projects on the basis of the argument that the consent supposedly given by students was not freely given and that the processing of biometric data in this case could not meet the requirements of necessity and proportionality.

Two right wing politicians involved in this pilot project reacted angrily to the positions put forward by the CNIL. The President of the PACA Region R. Muselier accused the French DPA of "being lost in the previous century" and having a "dusty ideology". The Mayor of the city of Nice C. Estrosi accused the CNIL of being "a State within the State" and expressed his determination to move forward with such tests in the future. The same politician accused the CNIL of being an "autonomous organ" disconnected from reality and the desires of citizens, and asked the French Prime Minister to review and downgrade the powers of the French DPA:

"We ask the government to reflect on the scope of intervention of the CNIL, to analyse its functioning, to determine if the concentration of as many powers, without any control, is desirable, if in the world other democracies also come up against this permanent censorship, if finally these ideological obstacles are likely to endanger our country and our fellow citizens".

It is interesting to note that shortly after these attacks, the Administrative Court of Marseille confirmed the CNIL's position.[19]

2. Voices Opposing the Use of FRT in Public Spaces

In sharp contrast to such positions, an important number of stakeholders (including some politicians in France[20]), have called either for a ban on "biometric mass surveillance" or for a more general ban on "biometric recognition in public spaces".

"Reclaim Your Face": Dozens of NGOs call for a ban on "biometric mass surveillance"

A large number of NGOs have launched a campaign calling for "biometric mass surveillance" to be banned, as well as launching a European Citizens' Initiative (ECI), which is the official petitioning tool the European Union puts at the disposal of citizens who want to organise and request new laws. For an ECI to be successful (and therefore lead the Commission to take action), the petition has to obtain 1 million signatures over a period of 12 months (this was extended to 17 months for this ECI due to the COVID-19 pandemic). Despite the fact that the petition has, at the time of writing this report, gathered only 70,668 signatures[21], the campaign has been successful in raising awareness about these important issues, yielding information, and intervening in the ongoing debates about the regulation of FRT and other biometric or biometrics-based techniques in Europe (and beyond).

[19] For this case and sources see T. Christakis, "First Ever Decision of a French Court Applying GDPR to Facial Recognition", *AI-Regulation.com*, February 27th, 2020.
[20] See for instance "Reconnaissance faciale : l'urgence d'un moratoire", *Libération*, December 17, 2019.
[21] See https://reclaimyourface.eu/why-eci/.

"Reclaim Your Face" defines "biometric mass surveillance" as: *"any monitoring, tracking, and otherwise processing of the biometric data of individuals or groups in an indiscriminate or arbitrarily-targeted manner".*

Facial recognition is considered as: *"a form of 'biometric mass surveillance' because it takes people's face data (which is a type of their biometric data) and uses it to watch and analyse them".*

EDRi, one of the NGOs that were involved at the beginning of this initiative, explains in a paper intended to justify the need for such a ban, this call to action requires that: *"EU Member States immediately halt all biometric processing that could amount to mass surveillance in public spaces, ensuring that both current and future deployments are included"*.[22]

In a more recent response to the European Commission AI adoption consultation, EDRi appears to be advocating for a general ban on remote biometric identification techniques in public places. They ask to:

"Comprehensively prohibit the use of remote biometric identification in publicly accessible spaces for any purpose, and implement a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces".[23]

These calls for a ban on "biometric mass surveillance" have been espoused by such political movements as the Greens in the European Parliament[24] and even, it seems, by the new government in Germany.

Germany: New coalition calls for "biometric recognition in public spaces to be excluded under European law"

The previous German government, under the leadership of the CDU/CSU, deployed certain FRT pilot projects in a number of public places, such as train stations. The experiment conducted by the Federal police at the Berlin Südkreuz Station (to be analysed later in our study) attracted a great deal of attention and criticism. In late 2019, the German Federal government was planning to introduce a specific legal basis for the use of FR by the police, by amending the Bundespolizeigesetz (Federal Police Act). This amendment created a great deal of controversy, however, and was never implemented.[25]

2021 saw the new coalition bring to power the political parties that had been most critical of facial recognition, in particular the Greens and the FDP.[26] The coalition agreement adopted by the SPD, the Greens and the FDP in November 2021 states:

"Biometric recognition in public spaces as well as automated government scoring systems through AI are to be excluded under European law".[27]

[22] See EDRi : "Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States", May 2020.
[23] See EDRi submits response to the European Commission AI adoption consultation, August 3, 2021.
[24] See https://www.greens-efa.eu/en/campaigns/ban-biometric-mass-surveillance.
[25] See DEUTSCHER BUNDESTAG, "Kontroverse um Einführung einer automatisierten Gesichtserkennung", January 30th, 2020.
[26] See O. Nolan, "New German government to ban facial recognition and mass surveillance", *Euractiv*, November 26th, 2021.
[27] Koalitionsvertrag, November 2021, p. 109, available at 18.

Aside from these political positions, it is important to emphasise that European independent authorities have also called for a "general ban" in this field.

EU Data Protection Authorities call for "a general ban"

In June 2021 the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) published a Joint Opinion on the draft AI Regulation proposed by the European Commission. In this Opinion the two European watchdogs appear to be adopting a particularly strong position, to the extent that they:

"**call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals - in any context".**[28]

As such, this paragraph seems to call for "a general ban" on any use of FRT in publicly accessible spaces "in any context", which seems to also logically include, for instance, face verification/authentication cases. However, to the extent that in the previous paragraph the Joint Opinion is only focused on "real- time remote biometric identification in publicly accessible spaces for the purpose of law enforcement", and thus characterises the exceptions proposed by the Commission in this regard as "flawed", it remains to be seen whether the EU data protection authorities only wanted to focus on this very specific use case or indeed intended to call for "a general ban" on *any use* of FRT in publicly accessible spaces "in any context".

3. First reactions of the Council and the European Parliament

Following the introduction of the AI draft regulation, and its accompanying important proposals on the use of remote biometric identification systems in public spaces,[29] the two EU legislators, the European Council and the European Parliament have begun their legislative work. It is interesting, therefore, to observe how these institutions and bodies have so far reacted to these proposals.

EU Member States: Assessing the impact of the proposals on "Remote Biometric Identification" (RBI)[30]

As the European Commission noted in the draft AI regulation Impact Assessment Study, in advance of publishing the draft, certain countries (e.g. France, Finland, the Czech republic and Denmark) have claimed that:

"the use of remote biometric identification systems in public spaces might be justified for important public security reasons under strict legal conditions and

[28] Joint Opinion of the European Data Protection Supervisor and the European Data Protection Board of 22 April 2021 regarding the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), June 18, 2021, para. 32. Emphasis by the EDPB and the EDPS.

[29] For the exact content of these proposals see *supra* notes 1-3.

[30] For the definition of "RBI" in the draft EU AI Regulation see note 3.

safeguards".[31]

Following the publication of the draft AI Act, the Council has yet to agree on its basic approach to this issue (and the AI Act in general). However, the JHA/law enforcement community from some EU Member States was questioning the impact of the legal proposal on their work. [32]

Evolutions at the European Parliament

The various, relevant Committees of the European Parliament are actually working intensively on defining their positions with regard to the AI Act. The official rapporteurs of the European Parliament's Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, MEPs Brando Benifei (S&D) and Dragoș Tudorache (Renew), have not been able to agree on a common position on the issue of RBI in their draft report on the AI Act published on April 20, 2022.[33] In the past, the two rapporteurs seem to have expressed conflicting views on the issue. Brando Benifei has been quoted as saying:

"Personally, I'm for a ban [on facial recognition]",[34] *while Dragos Tudorache has stated: "I don't believe in an outright ban. For me the solution is to put the right rules in place".*[35]

Other MEPs who have considerable influence as regards this topic, have also expressed conflicting views. For instance, Axel Voss, an EPP member of the Legal Affairs Committee, stated that "facial recognition should be allowed with safeguards in place"[36] and that "a complete ban of facial recognition disregards the benefits such technology can have, for example when tracking down criminals or even as part of other use cases such as training autonomous vehicles to recognise humans".[37] On the other side of the spectrum, the shadow rapporteur Sergey Lagodinsky (Greens) has recently introduced an amendment in the report of the Legal Affairs Committee, the purpose of which is to greatly extend the ban on RBI proposed by the Commission by proposing a complete ban on *"the use of remote biometric identification systems in publicly accessible spaces"* (the kind of language which envisages a complete ban in relation to both public and private actors) and by retracting all the exceptions proposed by the Commission for the benefit of law enforcement authorities.[38]

[31] See the Impact Assessment Study, page 18.

[32] During a JHA/law enforcement workshop held on 30 September 30, 2021, for instance, there was "a clear call" from several EU Member States "to better understand the short, medium and long term implications of the proposal and especially of some of its key aspects (e.g. the prohibition of real time remote biometric identification in public places for law enforcement purposes)". Restricted Council documents seen by the authors.

[33] See the joint draft Report on the AI Act by Rapporteurs Brando Benifei and Ioan-Dragos, Tudorache of the Committee on the Internal Market and Consumer Protection (IMCO) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE), 20 April 2022, where it is stated that "the draft Report contains the points on which the co-Rapporteurs could easily agree…".

[34] See M. Heikkilä, Politico AI: Decoded, July 21st, 2021.

[35] See Europe's bid for AI standard faces long road, EU lawmakers say, *Euractiv*, February 16th, 2022.

[36] Ibid.

[37] See L. Bertuzzi, "Facial recognition technologies already used in 11 EU countries and counting, report says", *Euractiv*, October 26th, 2021.

[38] See Amendment 534 proposed by Sergey Lagodinsky.

IV. DEFINITIONS: UNDERSTANDING WHAT IS MEANT BY "FACIAL RECOGNITION", "BIOMETRIC DATA", "BIOMETRICS-BASED DATA"...

Our study covers both "facial recognition", as understood in its traditional sense (and closely associated with the concept of "biometric data") and "face analysis", where strictly speaking no "facial recognition" takes place, but where there is use of what is defined, via an emerging new term, as "biometric-based data" (see below). Before explaining the scope of our study, it is therefore important to dive into the important issue of how these AI-related terms are defined. As we will see, the existing definitions are not entirely satisfactory, and this has encouraged various stakeholders to introduce new terms and categories, which may resolve certain problems but is also accentuating the overall terminological confusion.

1. The Starting Point: "Facial Recognition", "Biometric Data" and "Specific Technical Processing"

We need to stress from the outset that the term "facial recognition" *has not been defined* in any EU data protection law instruments. Neither the GDPR, nor the LED, nor any other binding instrument have proposed a definition for this term. As for the draft EU AI Regulation, it does not intend to define "facial recognition" either. It focuses instead on the term "Remote Biometric Identification" (RBI), a term which is at the same time narrower[39] and broader[40] than "facial recognition".

This lack of definition of "facial recognition" contributes to the problems that arise in the public debate as a result of conflating different FRT functionalities and uses, and occasionally leads to "one-size-fits-all" approaches being taken. It is also problematic in terms of the protection of rights and the establishment of adequately focused legal and regulatory safeguards. The only definitions that we can find come from DPAs, such as the French CNIL, who closely associate the concept of "facial recognition"[41] with the concept of "biometric data".

[39] "RBI" is a specific *application* of Facial Recognition Techniques. As the Commission explains in Article 3(36) and Recital 8 of the draft, the notion of RBI system as used in this Regulation "should be defined functionally, as an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used". This shows that "RBI" does not cover the "Face Verification" functionality of facial recognition. See our classification in Part 2 of the MAPFRE Reports.

[40] "RBI" is also broader, because it potentially includes remote biometric systems using elements other than faces, such as gait or voices.

[41] In 2012 the EDPB's predecessor defined, in a more general way, facial recognition as "the automatic processing of digital images which contain the faces of individuals for the purpose of identification,

Definition of "facial recognition" according to the French DPA (2019)

In a general Opinion on Facial recognition published in November 2019, the French CNIL defined this term in the following way:

> *"Facial recognition is a* ***probabilistic software application*** *that can automatically recognise a person based on their facial attributes in order to authenticate or identify them.*
> ***Facial recognition falls into the broader category of biometric technology****. Biometrics include all automated processes used to recognise an individual by quantifying their physical, physiological or behavioural characteristics (fingerprints, blood vessel patterns, iris structure, etc.). The GDPR defines these characteristics as "biometric data", because they allow or confirm the unique identification of that person.*
> *This is the case with people's faces or, more specifically, their technical processing using facial recognition devices: by taking the image of a face (a photograph or video), it is possible to produce a digital representation of distinct characteristics of this face (this is called a "template"). This template is supposed to be unique and specific to each person and it is, in principle, permanent over time. In the recognition phase, the device then compares this template with other templates previously produced or calculated directly from faces found on an image, photo or video. "Facial recognition" is therefore a two-step process:* ***the collection of the face and its transformation into a template, followed by the recognition of this face by comparing the corresponding template with one or more other templates".***[42]

The link between "facial recognition" and "biometric data" is very important, because not only the GDPR but *all* existing European data protection instruments define "biometric data" in exactly the same way, putting emphasis on the criterion of *"specific technical processing"*.

"Specific technical processing": The definition of "biometric data" in EU data protection Law

Article 4(14) of the GDPR, Article 3(13) of the Law Enforcement Directive (LED) and Article 3(18) of Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by EU Union institutions, *all* define "biometric data" in exactly the same way:

> *"'****biometric data'*** *means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".*

This definition places emphasis on the functional/technical element of *"specific technical processing"*, which has certain important consequences.

Let's begin by explaining that the term "biometric data" does not refer as such to the physical, physiological or behavioural characteristics of a natural person: a face is not "biometric data" under EU data protection law. The *digital*

authentication/verification or categorisation of those individuals". See Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, March 2012, at 2.

[42] CNIL, "Facial Recognition: For a debate living up to the challenges", November 2019. Emphasis by the CNIL.

processing of a face (for instance a facial image) could, nonetheless, result in biometric data but only under certain specific circumstances. This is where the difficulties begin, because of this ambiguous definition of "biometric data" in EU data protection law.

Indeed, it could be argued that not all of the "data processing", in relation to the physical, physiological or behavioural characteristics of a natural person, which permit the identification of such a person, should be considered "biometric data" under the existing definitions of the GDPR and the LED. To the extent that such "processing" "relates to an identified or identifiable natural person", it certainly meets the definition of "personal data" under the GDPR[43], and should be protected as such. The processing of people's photos and facial images, for instance, which enables to identify them, constitutes processing of "personal data". However, based on the definition above, it could be argued that, if this processing of personal data does not involve any *"specific technical processing"* "allowing the unique identification of a natural person" (biometric processing), then it does not fall within the category of "biometric data". As Recital 51 of the GDPR indicates:

> *"The processing of photographs*[44] *should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person".*

The problem with this definition of "biometric data" is that the fundamental criterion of "specific technical processing…allowing the unique identification of a natural person" is not explained anywhere in the European legal instruments. Based on existing interpretations provided by DPAs such as the CNIL, it seems, nonetheless, that the *"specific technical processing"* in question **involves the creation of biometric templates which could be used for face matching** in order to identify a person. So, when the facial images are prepared for face matching, "allowing the unique identification" of a natural person, biometric processing does take place, the outcome of which is the creation of "biometric data".

Before continuing our analysis of "facial recognition", it is important to explain why this definition of "biometric data" in existing EU Law is problematic and confusing.

Lost in translation?
Why this definition of "biometric data" is problematic

This definition of "biometric data", as well as the legal regime(s) reserved for such a form of data in EU law, are confusing[45] for at least three reasons.

First, it is hard to understand why Article 4(14) of the GDPR and Article 3(13) of the LED end with the words "*such as facial images",* when it appears

[43] According to Article 4(1) of the GDPR: "'**personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly…".

[44] The GDPR does not explain what the term "photographs" refers to. Is it the same as the term "facial images" in Article 4(14)?

[45] The definition is indeed so confusing, that people could challenge the interpretation proposed here and could argue that the issue is yet to be resolved through legal processes or litigation.

that *not all facial images* constitute "biometric data"*; only* those that are prepared for face matching using "specific technical processing".

Second, arguing that a "raw" facial image does not classify as biometric data, but a biometric template derived from it does, is somewhat weird, since technically the "raw" facial image most often contains more information about a person than the biometric template.

Third, things get even more confusing when one bears in mind that the category of data called "biometric data" does not benefit from any specific legal regime or protection (other than that accorded *to all* "personal data") under EU data protection law. Indeed, the specific protections accorded by Article 9 of the GDPR or Article 10 LED to the "processing of special categories of personal data" *only* apply when "***processing* of biometric data for the purpose of uniquely identifying a natural person**" takes place. In other words, the "biometric data" (as defined above) must be *processed* for the finality of identifying a person, in order for the special protections of these articles to apply. In order to explain this as simply as possible, we have distinguished three main scenarios (in which the law applies differently in each case):

(1) A facial image (photo or video) constitutes "personal data" under the GDPR/LED and must be protected as such;

(2) A facial image which is transformed into a biometric template, which could be used in the future for face matching in order to identify a person, constitutes "biometric data" under the GDPR/LED – but this does not automatically result in any special protection other than that which applies to "personal data" in general;

(3) If the biometric template mentioned in (2) is *effectively processed* in order for face matching to be carried out for the purpose of identifying a natural person, *then* the special protections of Article 9 of the GDPR and Article 10 LED apply.

This definition of biometric data differs from previous definitions proposed by various institutions, which have not included the *"specific technical processing"* element.[46] It appears that this element was only added as a result of a political agreement in the Council in June 2015, when its General Approach was adopted.[47] A possible explanation for this late addition was the willingness of EU Member States at the Council to exclude the processing of law enforcement and other databases from the special protections accorded to the "processing of biometric data" by Article 9 of the GDPR and Article 10 LED. As Els Kindt explains, databases which contain facial images, and which *have not been* subject to biometric processing, would *not* be considered databases that contain biometric data or biometric databases. The processing of such databases would therefore *not* be subject to *specific protective rules* for biometric data processing, other than the data protection rules which apply to all personal data. As Kindt argues, this is the case despite the fact that the construction of such databases is the pre-condition for biometric identification, involving significant risks for the fundamental rights

[46] See for instance C. Jasserand-Breeman, "Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?", PhD Thesis, University of Groningen, 2019, at 46-54. As she notes (on page 52): "most of the proposed regulatory definitions for the term 'biometric data' do not mention the technical process of extraction of biometric information and its transformation into a digital template".

[47] See for instance the critical analysis by E. J. Kindt, "Having yes, using no? About the new legal regime for biometric data", *Computer Law and Security Review*, Volume 34, Issue 3, June 2018, p. 12.

and freedoms of the data subjects.[48]

Despite these ambiguities, the draft AI Act, published by the European Commission in April 2021, espouses the traditional definition of biometric data in Article 3(33), while insisting on the need to interpret the "notion of biometric data used in this Regulation" in "line and consistently" with the notion of biometric data as defined in the GDPR and the other EU data protection texts.

However, as we will see, the ambiguities surrounding the concept of "biometric data" have led some lawmakers to suggest that an entirely new term, "biometric-based data", should be introduced, in order to resolve certain difficulties that have arisen as a result of references to the traditional term "biometric data" in the AI Act...

Reserving the concept of "biometric data" to data resulting from *specific biometric processing*, means that, according to existing EU data protection law, facial image processing systems which do not involve such biometric processing and/or do not "allow or confirm the unique identification" of a natural person should not be considered as being "biometric data" processors, nor as being "facial recognition" systems. The CNIL insisted on this point in 2019.

CNIL: "Facial recognition is not synonymous with "smart" video"

In its 2019 Opinion on facial recognition the French DPA stressed the following:

"CCTV systems can film people within a defined area, in particular their faces, but they cannot be used as such to automatically recognise individuals. The same applies to simple photography: a camera is not a facial recognition system because photographs of people need to be processed in a specific way in order to extract biometric data.

The mere detection of faces by so-called "smart" cameras does not constitute a facial recognition system either. While their use also raises important questions in terms of ethics and effectiveness, digital techniques for detecting abnormal behaviours or violent events, or for recognising facial emotions or even silhouettes, are not typically biometric systems".[49]

It seems clear then that, for the French DPA, "facial analysis" systems that enable the processing of faces (for instance for statistical purposes) but do not involve biometric processing and face matching,[50] should not be considered as systems that process "biometric data" or conduct "facial recognition". This has been confirmed in practice, in a very interesting case in France, which is one of the "25 selected cases" that we have analysed *in extenso* during our study.

[48] See *ibid*, p. 11.

[49] CNIL, "Facial Recognition: For a debate living up to the challenges", November 2019.

[50] For more explanations about the term "face matching" see T. Christakis et al., "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification", May 2022.

The *Datakalab* Case: Mask detection in public spaces during the Covid-19 pandemic *does not* equate to processing of "biometric data"

Datakalab, a French start-up, was asked by the 'Régie Autonome des Transports Parisiens' (RATP) and by Cannes City Council to deploy its mask detection tool to help monitor mask wearing adherence during the Covid-19 pandemic. The system was not intended to be used to sanction people for not wearing masks. It was instead intended to be used for pure statistical purposes, to help the data controllers implement preventive actions in order to improve mask adherence. From a technical point of view, Datakalab claimed that its system *is not a facial recognition tool* as it is not designed to identify people. The French DPA accepted the argument that the system was "not intended, nor technically capable, of identifying individuals", and was **"not intended to process biometric data"** since it did not generate a biometric template.[51] However, the CNIL did consider that the system **involved the processing of personal data** and thus concluded that the system needed a proper legal basis under Article 6 of the GDPR.

It is interesting to note that the CNIL is currently working on a broader Opinion about an adequate legal framework for the use of *'intelligent' cameras* in public spaces in France. This draft specifically excludes the use of 'biometric recognition' systems. It stresses, once again, that 'intelligent' or 'augmented' video devices that perform functions similar to Datakalab, even if they are used for purely statistical purposes and not for the purpose of identification, do process personal data and are thus subject to EU data protection regulation. The CNIL emphasised the following:

> *"Insofar as 'augmented' video devices capture and analyse data, in particular images that would make it possible to identify individuals, their use and the data processing they involve must comply with all the regulations applicable to personal data (i.e. the GDPR and the Loi Informatique et Libertés).*
>
> *It should be remembered that, even if the images are anonymised, or even destroyed, very quickly after they are captured and analysed, these operations constitute processing of personal data if the images contain people".* [52]

European DPAs seem to agree that, after all, the key issue is whether the system generates a biometric template in order to assist with the identification of an individual; if so, it should be considered as being "intended to process biometric data".

The EDPB adopted the following position in this respect in January 2020:

[51] See for instance CNIL, Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, para. 8. Our translation. For a more general view, see our analysis of the Datakalab case in T. Christakis (et al.), "Mapping the Use of Facial Recognition in Public Spaces in Europe – 25 Selected Case Studies", forthcoming.

[52] See "Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics : la CNIL lance une consultation publique", January 14th, 2022.

The three relevant criteria according to the EDPB

In a guidance published in January 2020 the EDPB went at lengths in trying to explain the concept of *"biometric data"* and the threshold of applicability of Article 9(1) of the GDPR, on the processing of biometric data. The EDPB stated the following:

> *"To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person [...]". The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.*
>
> *In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed "for the purpose of uniquely identifying a natural person".*
>
> *To sum up, in light of Article 4.14 and 9, three criteria must be considered:*
>
> *- **Nature of data**: data relating to physical, physiological or behavioural characteristics of a natural person,*
> *- **Means and way of processing**: data "resulting from a specific technical processing",*
> *- **Purpose of processing**: data must be used for the purpose of uniquely identifying a natural person".*[53]

Despite all these clarifications, one may retain the impression that the approach of the GDPR in this field is not satisfactory.[54] Things may become even more complicated in the future, when one takes into consideration various current attempts to amend existing definitions, or introduce new ones – attempts towards which we will now turn.

2. Challenging the Criterion of "Identification"?

Recently, as a result of discussions within the French Presidency of the European Council on the draft AI Act, amendments have been proposed which openly seek to amend the traditional definition of biometric data in EU data protection law, with a view to entirely removing the criterion of *"identification".*

[53] EDPB, Guidelines 3/2019 on processing of personal data through video devices, January 29, 2020 at 18.
[54] See for instance the criticism formulated by E. J. Kindt, "Having yes, using no? About the new legal regime for biometric data", *Computer Law and Security Review*, Volume 34, Issue 3, June 2018, at 11-24.

French presidency amendments to the AI Act: An effort to remove "identification" from the traditional definition of biometric data?

In April 2022, the French presidency of the Council of the EU proposed a series of amendments to the AI Act including one amendment which aims to remove the criterion of identification from the "traditional" definition of "biometric data". Here is the new text proposed by the Presidency for Article 3(33) of the AI Act:

"(33) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, ~~which allow or confirm the unique identification of that natural person~~, such as facial images or dactyloscopic data".[55]

It is not clear why the French Presidency is proposing such an important amendment to the traditional definition of biometric data. One reason could be that an effort is being made to address precisely the same problem in the draft AI Act that members of the European Parliament are trying to address by introducing an entirely new term (see point 3 below). However, the consequences of such an amendment, if accepted, could be significant as it is difficult to imagine how we could have a different definition of "biometric data" in the GDPR and the LED to that in the AI Act.

The attempts of members of the European Parliament to instead create an entirely new category called "biometrics-based data" appears equally interesting.

3. Creating a New Category called "Biometrics-Based Data"?

Following a similar proposal introduced at the Legal Affairs Committee of the European Parliament by the shadow rapporteur Sergey Lagodinsky (Greens),[56] the two lawmakers leading the European Parliament's negotiations on the EU's AI draft regulation have proposed introducing an entirely new category called "biometrics-based data".

Amendments proposed by the European Parliament's Rapporteurs include both "biometric data" and "biometrics-based data"

The official rapporteurs of the European Parliament's Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, MEPs Brando Benifei (S&D) and Dragoş Tudorache (Renew), proposed a series of important amendments in their draft report on the AI Act published on April 20. Contrary to the French Presidency's proposal, the two rapporteurs did not challenge the "traditional" definition of "biometric data" found in the GDPR and other leading European data protection instruments, but instead created ***an additional*** category called

[55] See the document obtained by POLITICO. Deletion of the original text present in the French Presidency's amendment.

[56] Amendment 484 submitted by Sergey Lagodinsky available here. Emphasis added.

"biometrics-based data". Indeed, in Recital (7) of the AI Act they agree with the Commission that "the notion of biometric data used in this Regulation is ***the same as that*** [in the GDPR and the other relevant European instruments] ***and should therefore be interpreted consistently with those provisions"***. However, immediately afterwards they add that:

> *"**Biometrics-based data** are additional data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person".*

In a more detailed (and entirely new) definition introduced by the rapporteurs in Article 3 (33a) of the AI Act they define this new category in the following way:

> *"**'Biometrics-based data'** means data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person, such as facial expressions, movements, pulse frequency, voice, key strikes or gait, which may or may not allow or confirm the unique identification of a natural person".*[57]

When comparing the traditional definition of "biometric data" with the "biometrics-based data" definition, the latter chooses the word "signals" instead of "characteristics" when referring to a natural person, and follows this with examples of signals (such as facial expressions, movements, voice, etc). More importantly though, the criterion of "identification" has been removed from the definition.

We understand that the *rationale* behind this proposal is as follows. Lawmakers seem to consider that the existing definition of "biometric data" (as explained above) is too narrow. They also seem to consider that its introduction in the parts of the AI Act dedicated to "biometric categorisation systems" and "emotion recognition systems"[58] results in a situation where the protections concerning the use of such systems do not apply if the systems do not allow the "unique identification" of the natural person concerned. As a result, lawmakers wish to introduce a new term, "biometrics-based data", which should replace the term "biometric data" in the "biometric categorisation systems" and "emotion recognition systems" definitions. The definition of this new term is very similar to that of biometric data, but differs from it in this respect: "biometrics-based data" may *or may not* allow the identification of a natural person. The requirement of "specific technical processing" nevertheless remains intact, although, once again, it is not defined in this new regulatory approach. A report which was used as the basis for these amendments explains however that:

> *"It is important to stress that there would still be the requirement of specific technical processing, i.e. a video showing a person who is*

[57] See the joint draft Report on the AI Act by Rapporteurs Brando Benifei and Ioan-Dragos, Tudorache of the Committee on the Internal Market and Consumer Protection (IMCO) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE), 20 April 2022, Amendment 64.

[58] Article 3(34) of the draft AI Regulation defines **"emotion recognition system"** as "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons **on the basis of their biometric data**", while Article 3(34) of the draft states that **"biometric categorisation system"** means "an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, **on the basis of their biometric data**". Emphasis added.

> *smiling would not amount to biometrics-based data, but the use of specific analytic tools that tell a smiling person from a person in a different mood would qualify as biometrics-based data".*[59]

While the intentions are understandable, the creation of a new category so similar to the original one might create further confusion in this field. Els Kindt had noted that, if one carefully reads the GDPR and other existing European data protection instruments, one may come to the conclusion that there are already four different categories and legal regimes for data that concern physical/biometric characteristics.[60] Would the addition of a fifth category bring us anywhere closer to clarity? One should also expect that this addition will in future raise questions about the exact boundaries between "biometric data" and "biometrics-based data", based on calls by civil society to apply the same kind of protections (including, for instance, those applied by the GDPR to "biometric data") to both categories. In the long run, this could lead to a reconsideration of the relevance of the definition of "biometric data" in the GDPR, and it being replaced by the broader, and more protective notion of "biometric-based data".

[59] See European Parliament, "Biometric Recognition and Behavioural Detection", Study requested by the JURI and PETI Committees", August 2021, at 68.

[60] E. J. Kindt, "Having yes, using no? About the new legal regime for biometric data", *Computer Law and Security Review*, Volume 34, Issue 3, June 2018, at 17-18.

V. SCOPE OF THE MAPFRE STUDY

Three observations should be made about the scope of our study.

1. Material Scope: "Facial Recognition" AND "Face Analysis"

First, we have decided that the scope of our enquiry should include **all systems used to process facial images captured in public spaces**. These systems can have different purposes. The most common purpose is **facial recognition**, which is used as a means of authentication (verification that a person is who he/she claims to be) or identification (finding a person among a group of individuals). However, systems that do not conduct facial recognition *stricto sensu* but instead detect facial emotions or violent intentions or which conduct "biometric categorization" also raise important questions in terms of law, ethics and effectiveness and might also create risks for the rights and freedoms of people in public spaces. Therefore, these techniques (as long as they involve **face processing**), are referred to as "**facial analysis**" techniques, and are also covered by this study. In other words, 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 where there is neither "face recognition" nor "face analysis"**, such as general video surveillance or the processing of "biometrics-based data" other than face processing (such as voice, gait or non-facial behavioural recognition).

In the "Classification Table" presented in Part 2 of our study, we explain extensively the concept of "facial processing" and we identify three main facial processing system functionalities (verification, identification, and face analysis), each of which have a number of applications, which cover different situations and give rise to different types of risks, depending on a number of factors.

2. "Public Spaces"

A second issue that needs to be clarified in relation to the scope of our study involves spaces where FRT are used. Our study only concerns FRT deployments in public spaces and does not cover the use of FRT in private spaces (for instance, so that a user can unlock a phone or enter a private building), or online (for instance, so that an online service can be accessed).

For the needs of this research our starting point is the definition of "publicly accessible spaces" as it appears in Recital 9 of the draft European Commission's AI Regulation:

> *"For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in*

> *question is privately or publicly owned. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand".*

Taking into consideration the use cases that we have examined it is possible to distinguish, nonetheless, three subcategories for the needs of our presentation:

- **Open space**: accessible by default to anybody unconditionally, for instance streets, train stations, shopping centres, supermarkets, etc. Identification is not required to access such open spaces[61], where users remain in principle fully anonymous.
- **Restricted space**: accessible by default to anybody subject to conditions[62] (valid ticket, meeting the age restriction, etc.), for instance stadiums, cinemas or theatres. A user must demonstrate that he/she is authorised to access the space (for instance by presenting a ticket), but identification is not required in principle,[63] except in certain specific spaces[64] or circumstances.[65]
- **Closed space:** accessible only to a limited / fixed group of people (e.g. schools).[66]

3. Geographical Scope: EU Member States and the UK

Finally, with regard to the *territorial scope* of our study, we have decided to include cases that originate not only from EU Member States but also from the UK.

[61] Note, nevertheless, that identification might be used to exclude certain users (for example users who appear in a list of those people who have been banned and are prohibited from accessing a venue such as a supermarket – see the "MERCADONA" use case).

[62] "Subject to conditions" does not necessarily mean "subject to systematic control" (this depends on how access control is implemented and depends on the context).

[63] As mentioned above, identification may nevertheless be used to exclude certain users (e.g. to prevent those who have been banned from entering a stadium).

[64] For instance, airports are accessible by default to anybody, but identification is required at the boarding Gates.

[65] For instance, users who have a season ticket for a stadium, or an annual subscription for a theatre must identify themselves.

[66] It is debatable whether such a "closed space" should be considered a "publicly accessible space". However, we would prefer to keep "closed spaces" such as schools within the scope of this study for a number of reasons, including the fact that schools are, in principle, accessible by default to all children due to their having the right to an education. Furthermore, our study of use cases in Europe, and the attempts to use FRT in several schools for various purposes (for instance in the UK, in Sweden and in France) highlights the benefit of keeping schools within the scope of this study.

This is due to a number of considerations.

First, the UK was until recently a member of the EU and several of the cases that we have examined were initiated before Brexit occurred. Despite the UK's withdrawal from the EU, its legal framework on the protection of personal data is still very close to the existing EU framework. This legal framework mostly consists of the UK GDPR, as incorporated into the law of the UK under the EU (Withdrawal) Act 2018 and amended by the DPPEC Regulations, and the DPA 2018, as amended by the DPPEC Regulations. As the European Commission stressed in its UK adequacy decision of June 2021:

> *"As the UK GDPR is based on EU legislation, the data protection rules in the United Kingdom in many aspects closely mirror the corresponding rules applicable within the European Union."*[67]

The second reason is that the use of facial recognition at the UK is much more common than in EU Member States. When it comes to what the draft AI Regulation calls "real time remote biometric identification" by law enforcement authorities, for instance, we will see that in Europe there is a kind of *de facto* moratorium, due to a number of reasons, the main exceptions being certain rare, GDPR and consent-based (due to the absence of adequate legal basis under the LED) "experiments". In the UK, in contrast, police have been using live facial recognition for years. Similarly, "large scale face matching" is being used by private actors such as supermarkets wishing to enforce banning orders on their premises, while similar attempts by EU Member States have often been stopped, as we will see, by DPAs. Including the UK in our study therefore permits us to have a much broader range of use cases and to make useful comparisons with regard to a number of issues, including the seemingly "flexible" attitude of the UK DPA, Information Commissioner's Office (ICO), in relation to the use of facial recognition, when compared with the approach of its EU counterparts.

[67] See here, Recital (16).

VI. METHODOLOGY

In order to conduct our study, and a result of diligent enquiry, we have been able to propose a "Classification Table" of the uses of facial recognition/analysis in public spaces (1) and create a detailed analytical framework for the study of the use cases (2). We then proceeded to select 25 use cases to which we applied this analytical framework (3) before proceeding to the comparative analysis, which focuses on the different use cases.

1. Classification Table

The first tool that we have elaborated is a "Classification Table" of the uses of facial recognition/analysis in public spaces. This classification table, which will be published soon, forming "Part 2" of our MAPFRE project, 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 in preventing the phenomenon of "lumping all the uses of facial recognition together" and therefore also preventing the "distortion" of the public debate, which was highlighted by the CNIL.

2. Detailed Analytical Framework

The second methodological tool that we have elaborated is a detailed analytical framework which includes several key questions that the A.I. Regulation Chair researchers have formulated for the study of each one of our "25 selected use cases".

The template for this analytical framework is presented in an annex to this paper. To summarise the template, it involves 3 series of questions:

The first part involves a series of questions on the facts and technical details of the use case. This includes the type of case (based on the classification table), the location and date, who is involved (data controller; systems used and vendors, etc), the general objectives of the data controller, a precise description of the FRT technique used, how the system was deployed and lastly, the important question of whether the FRT deployment involved the use of databases and if so, whether information was disseminated about these databases.

The second part of our analytical framework focuses on Human Rights and principles relating to processing of personal data. It starts with a series of questions aimed at identifying the exact legal basis invoked by the data controller, in an environment where both the GDPR and the LED in principle prohibit the processing of biometric data, save for a few exceptions. Further questions look at whether there have been legal challenges concerning this legal basis and if so, the outcome and positions of DPAs and Courts. The questionnaire then turns to the major issue of the assessment of necessity and proportionality, before posing a series of detailed questions about whether and how the various principles relating to processing of personal data (purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality) were respected during the FRT deployment. The questionnaire of course also includes questions about how the data controller tried to deal with the risks of potential bias or discrimination.

The third part of our analytical framework tries to identify whether any additional guarantees were offered by the data controller, focusing on issues such as accountability and transparency, whether a Data Protection Impact Assessment (DPIA) was conducted, and if it was published, whether there was a posterior evaluation of the effectiveness of the system (and if it was published) and a series of other important questions.

Finally, for each case study, we include a bibliography with links to the most important documents (including the DPAs' positions) concerning the case.

3. Selection of 25 Use Cases

The next step in our work was to apply this analytical framework in order to analyse in detail 25 interesting use-cases, covering the various functionalities and applications found in our classification table.

The selection of these 25 use cases, among the dozens of cases that involve the use (or projected use) of face recognition/analysis in public spaces in Europe, was dictated by a number of factors:

- The importance of the cases and their representativeness in terms of the different categories that appear in our classification table;
- The benefit or otherwise of comparing similar cases in different countries in order to identify whether there were any convergences or divergences between DPAs in dealing with these cases;
- The availability of information – a criterion that is particularly important when one takes into consideration the lack of transparency and very limited information available on some deployments of facial recognition in public spaces in Europe;
- The existence and availability of DPA positions on these cases – another particularly important criterion considering how difficult it is to determine whether DPAs in certain countries have been involved in the deployment of FRT in some way and, if this is indeed the case, how difficult it is to access their documents (which are made public, in certain countries, only after access to information requests have been submitted);
- The existence of Court decisions, evaluations reports and other interesting documents;

A Report that includes a detailed analysis of our 25 selected use cases, with the responses to the questions appearing in the "analytical framework" annexed to the present report, will be published by the AI.Regulation Chair researchers[68] immediately after Part 6 of our analytical reports series is published. Furthermore, in each subsequent report we will include a table with the relevant use-cases analysed against each FR functionality/application, as well as a focus on the most important results and conclusions concerning each case.

It should also be emphasised that, aside from these 25 "selected" use cases, we have extensively analysed a dozen of other important cases of FR deployment in public spaces in Europe, which are discussed in the reports to come, but for which we will not be able to include a final detailed analysis.

[68] See T. Christakis et al., "Mapping the Use of Facial Recognition in Public Spaces in Europe – 25 Selected Case Studies", forthcoming.

CONCLUSION & OUTLINE

We hope that our study will be useful not only to policy-makers, stakeholders, scholars and citizens who may be interested in the issue of facial recognition/analysis, but also any person interested in how major human rights and data protection principles, such as the principle of lawfulness, the principles of necessity and proportionality or other principles relating to processing of personal data, are interpreted. Indeed, during our research into how facial recognition/analysis systems are deployed in Europe, we have found a treasure of information including documents produced by data controllers, legal challenges introduced by civil society, positions of DPAs, judgments of national courts, articles published by scholars and journalists, and other very interesting material. We expect that all of this material will be of great interest not only in relation to the ongoing debates on the regulation of facial recognition/analysis, but also, more generally, in relation to our understanding of how the GDPR, the LED and European Human Rights Law apply to a number of important fields.

Taking into consideration the time required to assess these materials and to prepare our report, we have decided to publish it in 6 successive parts:

- This **first part** has focused on the general context and has explained the objectives, the scope and the methodology of our study, while also diving into the important problem of definitions;
- **Part 2** provides a detailed explanation of the different facial processing functionalities and applications in public spaces in Europe and proposes a classification table, with illustrations, examples and charts;
- **Part 3** presents a first ever detailed study on the use of facial recognition for authorisation purposes in public spaces in Europe;
- **Part 4** focuses on the use of facial recognition and "individual identification" in criminal investigations;
- **Part 5** is devoted to the important issue of large-scale face matching/identification (also called "real-time remote biometric identification" or "live facial recognition");
- And, finally, **Part 6** will discuss briefly the use of "face analysis" (which involves facial processing but does not involve the processing of biometric data) in public spaces in Europe and will then formulate a series of general conclusions and recommendations.

A Report that includes the detailed analysis of our 25 selected use cases, based on questions appearing in the "analytical framework" annexed to the present report will be published at the end.

ANNEX
ANALYTICAL FRAMEWORK FOR USE CASE ANALYSIS
MAPFRE Project

Name of the Case

Summary of the Case

I.
FACTS AND TECHNICAL DETAILS ABOUT THE USE CASE

1) Type:

Category X (Sub-category X)

(on the basis of the classification table)

2) Country:

3) Location:

National or Local level?

Specific city/cities? Specific events? Broader use?

4) Just a limited trial, temporary arrangement (i.e. during an event) or continuous use?

If temporary, were the procedures to dismantle the system (data erasure, camera removal, etc) defined?

5) When was it used?

Specific dates/time period?

Or it has been a permanent fixture since…

6) Who is involved?

- Who is the data controller? (Art. 4(7) GDPR). Who are the operators of the system?
- Is the operation of the system subject to specific additional authorisation? If so, by whom?

- What are the systems used & who are the vendors?
- Any info about why this specific system was chosen?
- Is the detailed specification and performance of the system available (for example do we know which datasets were used to generate the recognition model?)?

7) General objectives of the data controller

for instance: border control; the fight against crime; the denial of entry of banned persons at specific venues; passenger flow optimisation; etc

8) Describe the FRT technique used and provide basic technical details

9) Did the FRT deployment involve the use of databases?

If yes:

A. <u>Use of preexisting databases?</u>

- Explain which databases are typically involved
- Explain the logic by which people are included in or removed from the database
- Can people obtain information about their existence on a database (or have this verified by an independent authority) and can they request that this be removed if it transpires that this action is illegal? If yes, what are the mechanisms in place to do so?
- Has there been any challenge/criticism of the use of these databases?
- Have any DPAs or Tribunals taken a position on the use of this database?

B. <u>New databases?</u>

- Explain which databases are typically involved
- Explain the logic by which people are included in or removed from the database
- Can people obtain information about their existence on a database (or have this verified by an independent authority) and can they request that this be removed if it transpires that their presence is illegal?
- Has there been any challenge/criticism of the use of these databases?
- Have any DPAs or tribunals taken a position on the use of this database?

II.
HUMAN RIGHTS &
PRINCIPLES RELATED TO PROCESSING OF BIOMETRIC DATA

1) Lawfulness of processing: What is the legal basis for the FRT use? (Art 6§9&2 GDPR or 8&10 LED)

A. <u>"Explicit" consent? (art.9§2(a)GDPR)</u>

- Explain in more detail how consent was given
- Explain what alternative methods were put in place for those who do not consent to FR
- Has there been any challenge using consent as a legal basis by any applicants?
- Have any DPAs or Tribunals taken a position on the use of consent as a legal basis?

B. <u>Another legal basis for processing the data under Art 6§9&2 GDPR or 8&10 LED)?</u>

- Which one(s)?
- Was there prior consultation with the DPA? If so, what was the position of the DPA on the legal basis used?
- Has there been any challenge to this legal basis by subjects?
- Has any Court taken a position on using this legal basis?

C. <u>Specific authorisation by EU or Member State law?</u>

- A law (statute)? An administrative act? Which one?
- Has there been any challenge to this legal basis by subjects?
- Has any DPA/Court taken a position on using this legal basis?

2) Necessity & Proportionality

- What is the legitimate aim of the data controller?
- Have alternative solutions/less intrusive means been considered to achieve the same legitimate aim?
- Explain whether any arguments have been advanced about how the use of FRT compares with other means of achieving the same objective
- What arguments have been put forward to show that the impact on human rights will be limited when compared with the importance of the legitimate aim that is to be achieved?
- Was there any challenge to the necessity and/or proportionality in this

specific case?

- Has a DPA or Tribunal taken any position on the necessity and/or proportionality in this specific case?

3) Addressing and Mitigating Bias and Discrimination

- Have any arguments been put forward to show that the system will avoid bias/discrimination?
- Was there any challenge to/criticism of the system by NGOs/subjects concerning bias/discrimination?
- Has a DPA or Tribunal taken any position on the issue of bias/discrimination?

4) Purpose Limitation

- Have there been any specific guarantees (in addition to the general data protection law) provided by the data controller or the relevant specific legal framework that biometric data will not be used for purposes other than those that have been previously stated?
- Has there been any challenge by NGOs/subjects concerning purpose limitation?
- Has a DPA or Tribunal taken any position on the issue of purpose limitation?

5) Data Minimisation

- Were any specific guarantees given by the data controller or relevant specific legal framework concerning respect for the principle of data minimisation?
- Was there any challenge by NGOs/subjects concerning data minimisation?
- Has a DPA or Tribunal taken any position on the issue of data minimisation?

6) Data accuracy

- Were any specific guarantees given by the data controller or relevant specific legal framework concerning respect for the principle of data accuracy?
- Has there been any challenge by NGOs/subjects concerning data accuracy?
- Has a DPA or Tribunal taken any position on the issue of data accuracy?

7) Storage Limitation

- Were any specific guarantees given by the data controller or relevant specific legal framework concerning respect for storage limitation requirements?
- Has there been any challenge by NGOs/subjects concerning storage limitation?
- Has a DPA or Tribunal taken any position on the issue of storage limitation?

8) Integrity and Confidentiality

- Were any specific guarantees given by the data controller concerning respect for the principle of integrity & confidentiality?
- Has there been any challenge by NGOs/subjects concerning the principle of integrity & confidentiality?
- Has a DPA or Tribunal taken any position on the principle of integrity & confidentiality?

III.

ADDITIONAL DATA CONTROLLER GUARANTEES

1) Accountability & Transparency

- Did the data controller adopt any specific measures to clearly inform the data subjects about the data processing?
- Did the data controller adopt any specific measures to inform the data subjects about the means by which they may exercise their rights?
- Did the data controller publish or commit to publish a transparency report about the specific reason for using FRT?
- Has there been any challenge by NGOs/subjects concerning accountability/transparency?
- Has a DPA or Tribunal taken any position on the issue of accountability/transparency?

2) Data Protection Impact Assessment

- Did the data controller prepare a DPIA before undertaking the use case?
- If so, was the DPIA published? Is any information available concerning the methodology used for the DPIA?
- Did a DPA or Tribunal take any position on the issue of the DPIA?

3) Interaction with the DPA

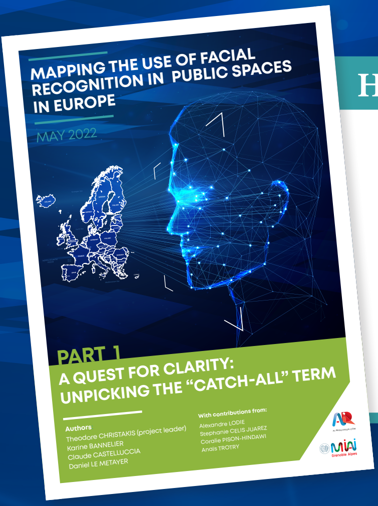
- Did the data controller notify the DPA of the projected use of the FRT, and communicate with them?
- Did the DPA issue an opinion on the specific use case (either following communication with the data controller or *proprio motu*?)
- If so, did the data controller follow the DPA's recommendation?

4) Human oversight

- Did the data controller provide for human oversight of the use of FRT? What exact form did this take? And how meaningful was it?

5) Evaluation of the effectiveness of the system

- Was there provision for an evaluation of the effectiveness of the FRT system and the specific way in which it was used? If so, was the assessment methodology described and documented?
- If so, was the system evaluated by the system providers? The data controllers? By independent third parties?
- Was the system evaluated in a lab or in the field (once deployed)? For how long? Is the system regularly evaluated while in use? Was a "sandbox" framework applied?
- What is the scope of the evaluation (the algorithm? the whole system?) and the evaluation criteria (false positive, false negative, discrimination metrics, etc.)?
- Will the evaluation report be published or be publicly accessible?
- Was any quantitative study carried out to evaluate the effectiveness of the FRT system with respect to its ultimate objectives (e.g. to reduce criminality, to facilitate criminal investigations, to search for missing people)? What were the results?
- What was the final outcome of the evaluation?
- Was fairness evaluated (i.e. accuracy across genders or different skin colour)?
- Was robustness considered (i.e. how easy it is to fool the system)?



MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE

MAY 2022

PART 1

A QUEST FOR CLARITY: UNPICKING THE "CATCH-ALL" TERM

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

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 1: A Quest for Clarity: Unpicking the 'Catch-All' Term", 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