AI-REGULATION.COM

Skopai
Deep Tech Insights

Landscape of Start-Ups Developing Facial Recognition

Analysis and Legal Considerations

Mathias Becuywe Tatiana Beliaeva Stephanie Beltran Gautron
Theodore Christakis Maéva El Bouchikhi Agnès Guerraz†

January 2022

This publication is dedicated to the memory of Agnès Guerraz,
co-founder and CEO of Skopai

The authors would like to thank Alexandre Lodie and Coralie Pison Hindawi for their contribution to this publication.

These statements are attributable to the authors only, and this publication does not necessarily reflect the views of the other members of the AI-Regulation Chair, Skopai, or any other partner organization.

This work has been partially supported by MIAI @ Grenoble Alpes, (ANR-19-P3IA-0003).

To cite this publication:

Becuywe, M., Beliaeva, T., Beltran Gautron, S., Christakis T., El Bouchikhi, M., Guerraz, A. *Landscape of start-ups developing facial recognition. Analysis and legal considerations,* AI-Regulation.com, Skopai.com, January 2022.

EXECUTIVE SUMMARY

Facial recognition technologies (FRTs) are on the rise, and so is the debate around their use and appropriate regulation.

In Europe, for instance, the European Commission published on April 21, 2021 its draft Artificial Intelligence (AI) regulation which includes several proposals on facial recognition. However, the proposed restrictions are deemed insufficient by numerous civil society actors calling for a global ban on the use of facial recognition in public spaces. The two major data protection authorities in Europe, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), are also jointly calling for such a ban.

Against this background, the AI Regulation Chair (MIAI, UGA) and Skopai, a Deep Tech and AI company that specialises in the compilation, analysis and classification of start-ups around the world, have engaged in a unique partnership in order to map the current landscape of start-ups developing facial recognition technologies. In this study, the two research partners have combined their talents in order to examine facial recognition technology-related products developed by start-ups worldwide.

This study therefore explores the main sectors, technologies and business models involved in facial recognition and questions the extent to which these companies take into account data protection rules and human rights. The study ends by focusing on how facial recognition start-ups have used their technology during the Covid-19 pandemic.

A total of 199 start-ups were identified, of which 130 were selected for this study; Skopai's AI tool was used to collect and process the data from publicly available internet sources. The quality and completeness of the data was verified by innovation experts, and further reviewed and analysed by the AI-Regulation team. The analysis includes a focus on the activities of certain start-ups in relation to specific issues; these are provided as case studies throughout the study.

The study showed that facial recognition start-ups are distributed globally across 36 different countries. Most start-ups' headquarters are located in the United States (20.9%), India (9.3%), the United Kingdom (7%), and France (6.2%). About half of start-ups (52.2%) focus exclusively on the development of facial recognition technology, but a significant number of them (47.8%) offer a broad portfolio of products. In terms of the technologies offered, face verification is by far the most common functionality (68%). Additionally, more than half of the start-ups (53%) provide face identification functionality, and 47% offer face analysis.

The majority of the start-ups analysed (60%) do not make any public statements about whether or how their products comply with existing safeguards on privacy and data protection. Some start-ups, however, argue that they are concerned about privacy and data protection, as a means of marketing themselves more effectively. They mostly achieve this by referring in general terms to the General Data Protection Regulation (GDPR) or other applicable legal texts. Yet, even among the start-ups that seek to convey a privacy-compliant public image, actual evidence of the legal requirements on data protection being implemented remains sparse.

The study ends with a focus on how facial recognition has been used during the Covid-19 pandemic. Although the available data does not permit us to confirm that the pandemic has been particularly favourable to the proliferation of facial recognition technology, around 20% of the analysed start-ups developed and/or adapted their facial recognition technology in order to offer Covid-19 related services. These include mask detection, using facial recognition to verify the identity of mask wearers, as well as crowd management, to limit overcrowding and verify that social distancing regulations are being respected.

CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
CAHAI	Ad Hoc Committee on Artificial Intelligence
CAHAI-PDG	Policy Development Group
CoE	Council of Europe
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EDRi	European Digital Rights
EU	European Union
FR	Facial Recognition
FRA	European Union Agency for Fundamental Rights
FRTs	Facial Recognition Technologies
GDPR	General Data Protection Regulation
LFR	Live Facial Recognition

LIST OF FIGURES

I. INTRODUCTION

This chapter introduces the study, its aim and scope, and the participating institutions – the AI Regulation Chair and Skopai. It describes methodology, data collection, and data analysis procedures, and outlines the schedule and structure of the report.

1.1. Background and objectives of the study

Facial recognition technologies (FRTs) are on the rise, and their development has been accelerated over the last few years. Facial recognition enables the identification of individuals by their facial characteristics. It collects, measures, analyses, and compares people's unique facial features. The applications of FRTs are vast, involving security measures, access control, surveillance, fleet management, computer entertainment, multimedia, and retail.

Along with the new opportunities provided by facial recognition, the ability to identify individuals by their face is closely related to regulatory, privacy, security, and data protection issues. There is an important debate going on worldwide about the "red lines" that should be fixed by regulators in order to avoid the human rights risks of the use of FRTs. In Europe, for instance, the European Commission published on April 21, 2021 its draft AI regulation[1] which includes several proposals to regulate the use of facial recognition[2]. However, these restrictions were deemed insufficient by civil society actors who issued an open letter calling for a global ban on facial recognition not only in the EU but also in other countries[3]. The two major data protection authorities in Europe, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), are also jointly calling for a ban on the use of biometric identification in public places[4].

Against this background, it is interesting to examine the FRT-related products developed by start-ups around the world and to determine to what extent these companies integrate data protection and other human rights considerations when they develop these technologies.

Which products are provided by facial recognition technologies? What are the main sectors, technologies, and business models of facial recognition? How do start-ups around the world developing facial recognition technology take into consideration data protection rules and human rights?

This study is set out to examine some of these questions while offering an analysis of the current landscape of start-ups developing facial recognition technologies as well as the sector in which they aim to be implemented. The study also aims to be useful in the debate about facial recognition regulation by focusing on start-ups as important innovators and providers of

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

[2] On the subject, see our articles on facial recognition regulation in the European Commission proposal:
- Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation
- Facial Recognition in the Draft AI Regulation: Useful Materials
- Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021.

[3] Algorithm Watch, "Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance", June 7, 2021.

[4] Team Ai-Regulation, "EDPS and EDPB's Joint Opinion on European Commission AI ACT Proposals", June 28, 2021.

novel facial recognition technologies, tools, and business models. It offers a snapshot of the facial recognition start-up ecosystem worldwide while offering a grid for analysing it through the prism of data protection law, as well as in light of the Covid-19 epidemic.

1.2. AI Regulation Chair

The Chair has been chosen by an international panel of experts to form part of the Multidisciplinary Institute on Artificial Intelligence (MIAI) created at the University of Grenoble Alpes, following a particularly competitive selection process commissioned by the French Government. Specialising in eight areas of expertise including facial recognition, its objective is to become a valuable contributor regarding the legal and regulatory questions raised by artificial intelligence and to contribute to national and international debates on these issues.

1.3. Skopai

Skopai is a Deep Tech and AI start-up. It offers, through its innovation intelligence platform, a full set of comprehensive and qualified real-time information on any start-up worldwide, including early-stage projects, with a particular focus on Deep Tech. The Skopai artificial intelligence (AI) platform specialises in the collection, analysis, and classification of start-ups. Using the validated methodology and machine learning algorithms, its objective is to help discover, monitor, and evaluate the most promising tech companies and innovation ecosystems across sectors, and facilitate decision-making processes by providing relevant, accurate, and reliable information in real-time.

1.4. Methodology

This study utilises the data on facial recognition start-ups provided by Skopai's AI tool. Skopai collects data from publicly available sources on the Internet. Start-ups are sourced from different types of aggregators including portfolios of incubators, accelerators, and investors, as well as information from media and newsletters. For each start-up, multiple sources, such as the start-up's website, social media accounts, company registers and databases, are inspected using web scraping bots. Processing the collected data, machine learning algorithms are trained to structure and classify information on the start-ups. They also automatically assign one or more predefined tags, which describe different aspects of a start-up related to its product, market, technology, and business model. The quality and completeness of the data are verified by innovation experts.

In order to identify start-ups that fit into the facial recognition domain, the assigned tags and the keywords, extracted from the start-up's website, have been used. Specifically, start-ups tagged with one or several of the following tags: *behaviourtech, computervision, image, imageprocessing, scantech, sensor, video, voicetech,* and one or several of the following tags: *biometrics, GDPR, idtech, legaltech,* and the tag *AI* were identified. Additionally, start-ups with keywords *face recognition* or *facial recognition* were included. Overall, 199 start-ups were identified within the framework of this study which covers developments till March 2021.

The start-ups were further reviewed by the AI-Regulation team of researchers to validate and select only those start-ups suitable for this study. Specifically, the start-ups that do not develop or offer facial recognition tools or no longer do so despite a biometric analysis of the person; start-ups whose website language does not allow for a thorough analysis; and start-up whose

information was not sufficient for an adequate examination of the topic were excluded from the analysis. For example, start-ups that exclusively analysed eye movement, or that were manufacturers of components necessary for the operation of facial recognition technologies, were excluded. Similarly, some start-ups that provide algorithmic video analysis in the broader context of smart city projects were excluded as none of their technologies included facial recognition. In the end, the list of selected start-ups included those that offer products or services using facial biometrics, whether for facial recognition or facial analysis purposes. Overall, this resulted in 130 start-ups being selected for this study (Annex I). Given the sector's fast development, it has to be acknowledged, however, that some start-ups may have not been included, despite the two co-authoring institutions' efforts to draw a comprehensive landscape.

The start-ups offer FR functionalities whose purpose is to identify individuals, verify their identity, analyse their behaviour, or to track them. The start-ups target both private and public actors. Using the information available on the websites, start-ups were classified based on different criteria, such as the tools they offer, sectors they serve, and their business types. We also tried to determine whether start-ups only offer facial recognition products or if they have a diversified product portfolio. Particular attention was paid to the start-ups' relationship to data protection, their marketing strategy regarding data protection obligations and the exact nature of their position with regard to national and/or international obligations. Special focus was also given to facial recognition technologies developed in the context of the fight against Covid-19. The classification was performed independently by researchers of the AI-Regulation Chair and the results have been jointly discussed between the participating institutions to ensure the validity and reliability of the study.

1.5. Schedule and structure of the report

The collaboration on this study between the co-authors started in December 2020. Research and analysis of the landscape of facial recognition start-ups took place between January and March 2021.

The report is structured as follows. After the introduction, a panoramic view of facial recognition start-ups is presented. Then the results of the analysis of start-ups according to their approach to data protection are provided. This is followed by the analysis of facial recognition start-ups in the context of the Covid-19 pandemic. Throughout the text, examples of representative start-ups are given to illustrate the results of the analysis.

II. A PANORAMIC VIEW OF FACIAL RECOGNITION START-UPS

This chapter presents an overview of facial recognition start-ups and analyses their proposed functionalities, sectors, technologies, and business models.

2.1. Functionalities

Facial recognition (FR) is often considered and described in general terms, although it covers a number of different techniques. For instance, according to the new European Commission (EC) legislative proposal for AI published on 21st April 2021, a remote biometric identification system:

“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. Considering their different characteristics and manners in which they are used, as well as the different risks involved, a distinction should be made between ‘real-time’ and ‘post’ remote biometric identification systems. In the case of ‘real-time’ systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay”.

This section analyses the sampled facial recognition start-ups according to the functionalities they provide (Figure 1).

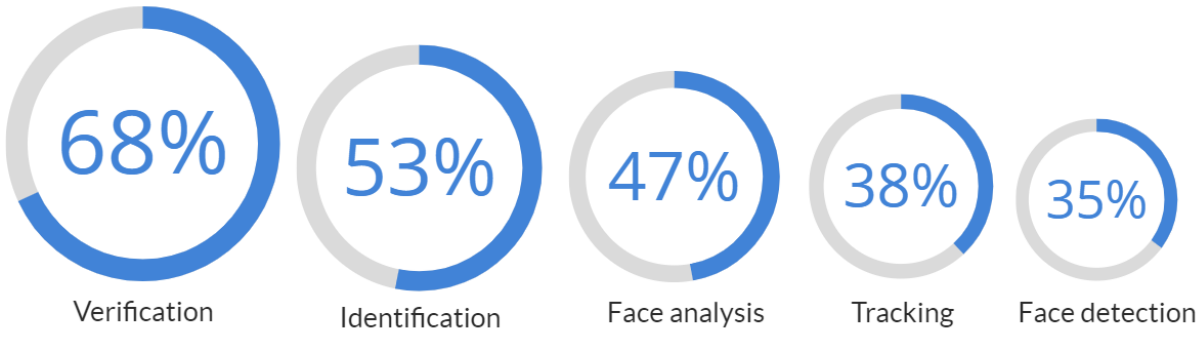

Figure 1. Solutions of facial recognition start-ups
Note: n=130.

The start-ups studied often offer several facial recognition functionalities. For the purposes of this study, the different categorisations are defined as follows:

- *Verification* consists of comparing the template of one face with another to check that the two templates correspond to the same face.
- *Identification* consists of extracting the template of a face and then comparing it against a database of pre-registered templates. The aim of this operation is to find the analysed face in the reference database and therefore to be able to identify it.
- *Face analysis* consists of an algorithmic analysis of facial features to extract certain information. Thus, it is possible to obtain an estimation of gender or age of a person analysed but also to detect emotions on a face scanned.
- *Tracking* consists of extracting the template of a person's face from an initial video source and then tracking that person as he/she moves through other video sources. This method does not necessarily lead to the matching of the analysed face with the identity of the person.
- *Face detection* consists of an automatic analysis of video sources to determine the presence of human faces.

Observing Figure 1 shows that verification is by far the most common proposed functionality (68%). This result may be explained by the fact that face verification is the most reliable facial recognition technique since it is deployed in a controlled environment, but also because it is the functionality where legal requirements are the most easily met (notably by relying on user

consent). Beyond verification, more than half of the start-ups (53%) provide identification functionalities, and 47% offer face analysis.

2.2. Sectors

The study revealed that the analysed facial recognition start-ups are distributed globally across 36 different countries. Most start-ups have their headquarters located in the United States (20.9%), India (9.3%), United Kingdom (7%), and France (6.2%) (Figure 2).

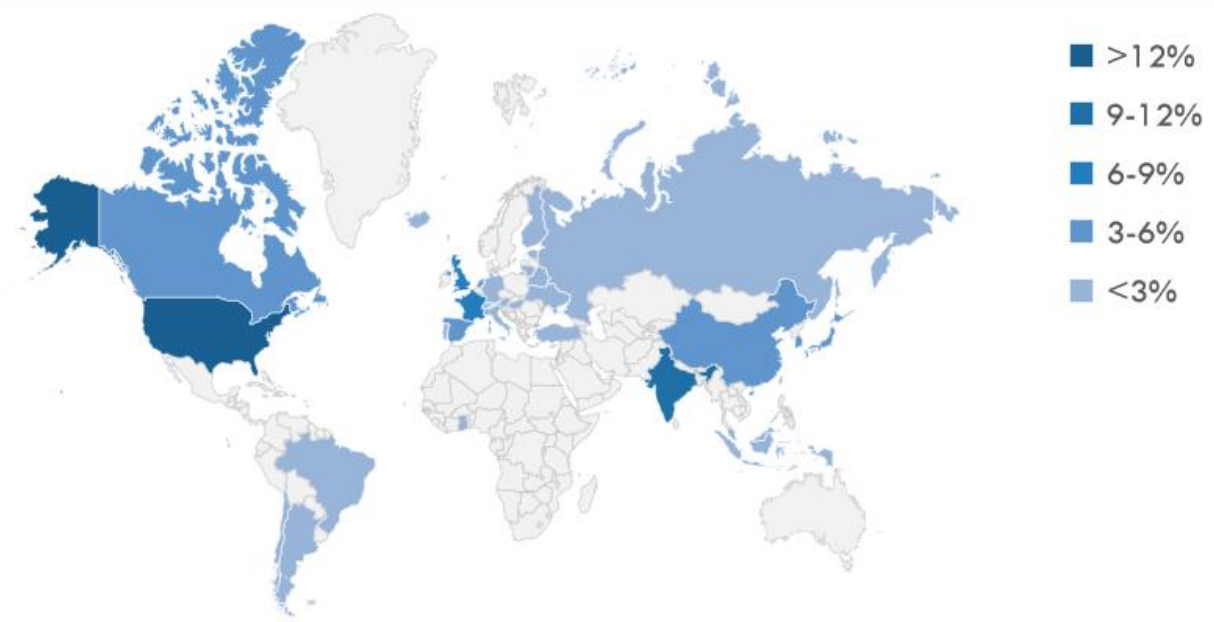

Figure 2. Geographical distribution of facial recognition start-ups
Note: n=130.

Apart from these four locations representing more than 40% of the facial recognition start-ups studied in this report, there is an increasing investment and interest in FRTs in China[5] and Latin America.

The analysis also revealed that the products and services offered by FR start-ups can be developed to meet a precise and specific use, in which case they are categorised in the corresponding sector. Alternatively, a start-up may offer a generic tool, the application of which is left to the customer's choice. The study thus provides an overview of sectorial applications of facial recognition products developed by start-ups (Figure 3).

[5] See "European Artificial Intelligence (AI) leadership, the path for an integrated vision", Policy Department for Economic, Scientific and Quality of Life Policies' Study, Directorate-General for International Policies, Laura Delponte (CSIL), September 2018, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf.

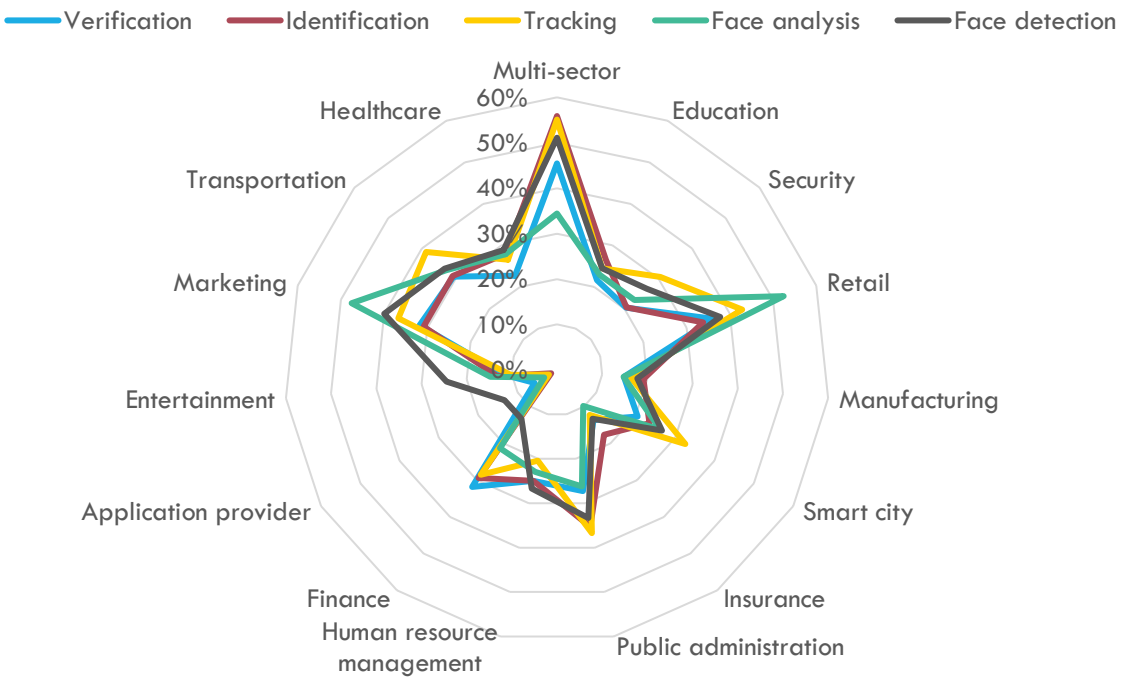

Figure 3. Products by sectors of start-ups
Note: verification: n=88; identification: n=68; tracking: n=49; face analysis: n=62; face detection: n=45.

The different categories and sectors are as follows:

- *The Multi-sector* category includes start-ups developing products that are not specific to a particular use. The solutions developed can, therefore, be used in different conditions, depending on the choice of the customer.
- *The Education* sector corresponds to products dedicated to the school environment. This can be solutions geared towards supporting a teacher or a student, but also products aiming to manage the security of schools or software to improve attention, or manage attendance, or fraud.
- *The Security* sector corresponds to products and services developed to meet the security needs of the state. These may include solutions enabling identification in the context of criminal investigations, but also military applications or applications used at border controls.
- *The Retail* sector covers products proposed for the management of shops. This includes solutions for securing shops, but also customer tracking programs for the purpose of analysing customer movements or as a part of fidelity programs.
- *The Manufacturing* sector covers products and services offered to manufacturers for the management of their production sites. This sector includes security products such as access control or surveillance of premises, but also solutions for monitoring compliance with procedures.
- *The Human resource management* sector includes both applications that enable facial analysis during a recruitment interview and products and services for workplace management. These include access control to buildings, video surveillance of workplaces and employee monitoring (e.g., break times, compliance with schedules).
- *The Insurance* sector includes start-ups that offer solutions to insurance companies mainly with the aim of securely identifying the customer and connecting to insurance

services, but also providing assessors with insights on fraud by detecting a range of facial cues.

- *The Smart city* sector brings together products implemented for the management of public space, whether by public authorities or private entities. It mainly concerns video surveillance of public spaces, enabling the identification of individuals, behavioural analysis, or monitoring of sanitary measures in the context of the Covid-19 pandemic.
- *The Public administration* sector corresponds to products offered to government authorities, with the exception of security or law enforcement operations. The purpose of this may be, for example, for the establishment of a digital identity or for the management of public buildings.
- *The Finance* sector covers products offered to financial institutions such as banks. The main use in this context is to provide stronger authentication of identity when carrying out financial transactions.
- *The Entertainment* sector concentrates on products designed for recreational use, such as filters and masks, or gaming applications, but also beauty and fashion applications that allow for an augmented reality facility. This sector also includes facial recognition used in casino and gambling places.
- *The Application provider* sector corresponds to start-ups that develop facial recognition interfaces to be integrated into applications by end developers.
- *The Marketing* sector covers products and services designed to provide marketing analysis, in particular by analysing the facial features of customers.
- *The Transportation* sector includes products and services intended for transport companies. It mainly covers two types of functions: video surveillance of boarding areas or transport vehicles, and applications designed to make boarding procedures more fluid.
- *The Healthcare* sector corresponds to products and services related to health. This may be for the management of healthcare facilities by means of automated video surveillance or access control to protected areas. It also covers health applications outside the health facilities, such as warning devices or aids for people with impaired vision for example.

Figure 3 illustrates that, in general, different tools follow a similar pattern when distributed across sectors. The graph also demonstrates that certain sectors favour a particular tool. For example, marketing and retail applications favour face analysis technologies to monitor customer reaction.

Though the graph and spectrum of analysis in Figure 3 permits an examination of the sectors in which facial recognition is most frequently used or intended-to-be used according to the current start-ups' development, another axis of focus applies a historical perspective and offers a deeper view of the trends and evolution of application of FR technologies (Figure 4).

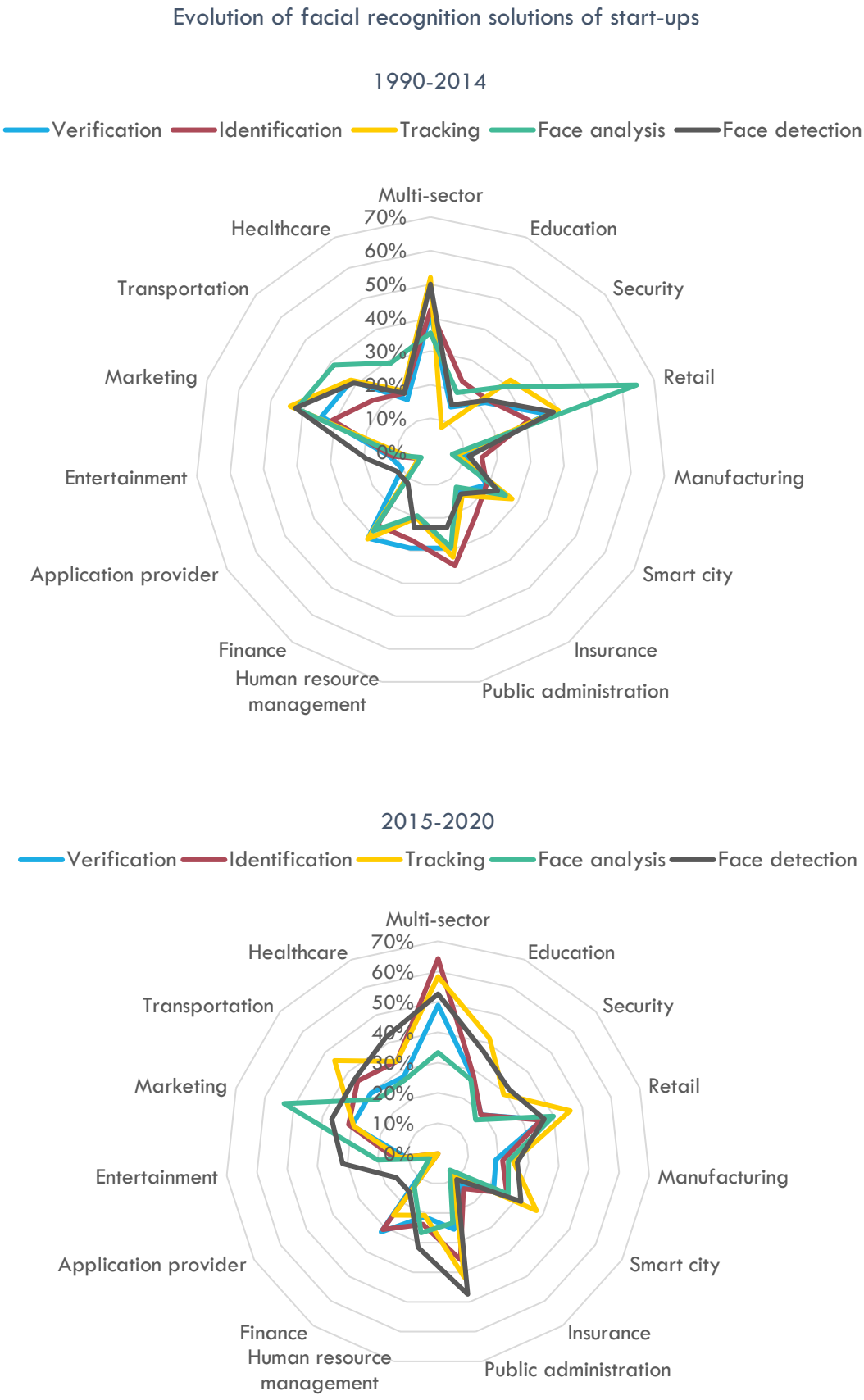

Figure 4. Solutions of start-ups, created between 1990-2014 and 2015-2020
Note: 1990-2014: verification: n=41; identification: n=26; tracking: n=25; face analysis: n=32; face detection: n=26.
2015-2020: verification: n=47; identification: n=42; tracking: n=24; face analysis: n=30; face detection: n=19.

The two graphs in Figure 4 highlight the sectorial developments of the start-ups founded between 1990 and 2020. For instance, it can be observed that face detection solutions were more sparely present in public administration between 1990 and 2014 (23%), whereas between 2015 and 2020, face detection in public administration increased to almost 50% of the studied start-ups. A more multi-sectorial approach emerged between 2015 and 2020 regardless of the solutions, thus allowing the technology to be deployed in a large variety of sectors and for a wide range of purposes. In contrast, during the earlier period, FR solutions seemed to predominantly target particular sectors and pursue specific purposes. These dynamics give an overview of the trends and movement of facial recognition technologies from a sectorial point of view.

2.3. Technology

Regarding technologies, the analysis of start-ups revealed that they can be divided into two groups. While some start-ups specialise in facial recognition technologies development only, others develop FR in a broader context while offering a diverse variety of other technologies (Figure 5).

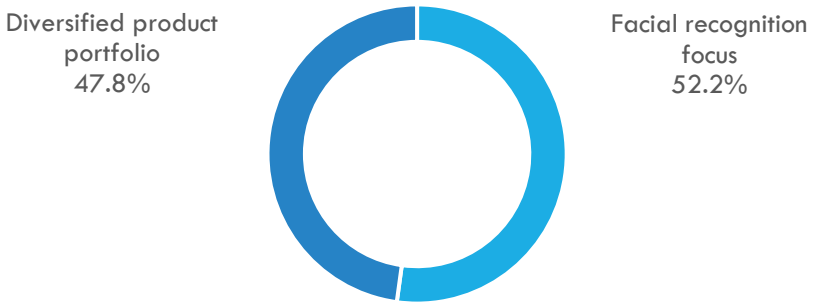

Figure 5. Technologies of facial recognition start-ups
Note: n=115.

The two different categories can be described as follows:

- *Diversified product portfolio* start-ups do not limit their offer to facial recognition applications and propose a wider range of technologies. They offer a broader technological environment that includes other applications, which can be combined with each other or with analysis services. Such offers include, for example, 3D reconstruction, graphics, asset management, cloud management, edge computing, predictive maintenance, big data analysis, biometric data management, consulting services, and other tools.
- *Facial recognition focused* start-ups concentrate their offer solely on facial recognition applications, and do not include other technologies. It should be noted that this includes the entire chain relevant to the operation of facial recognition, such as the creation and hosting of databases or the supply of relevant devices such as cameras.

Figure 5 shows that about half of start-ups (52.2%) focus exclusively on the development of facial recognition although a significant number of start-ups (47.8%) offer a broad portfolio of other products and technologies. The offer of multiple tools by start-ups may raise certain legal issues such as the reuse of collected data or the possibility of categorising individuals by mixing up the results of various technologies.

Figure 6 presents the various functionalities deployed by start-ups, depending on their focus area whereas Figure 7 describes the sectors in which their products are used.

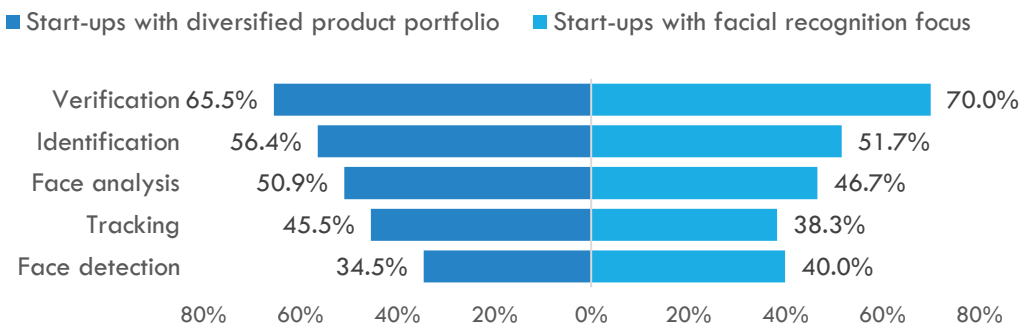

Figure 6. Solutions of start-ups with diversified product portfolio and start-ups with facial recognition focus
Note: diversified product portfolio: n=55; facial recognition focus: n=60.

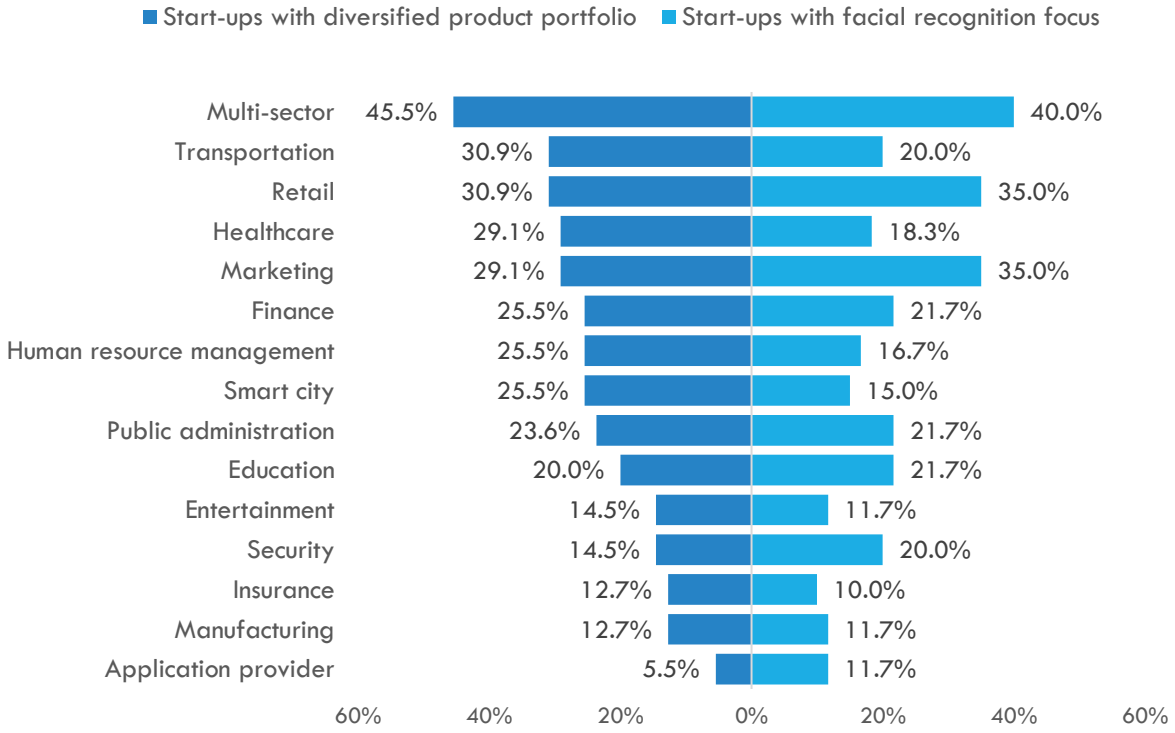

Figure 7. Sectors of start-ups with diversified product portfolio and start-ups with facial recognition focus
Note: diversified product portfolio: n=55; facial recognition focus: n=60.

The study found that most start-ups, regardless of whether they focus solely on FRTs or have a diversified product portfolio, are similar in terms of solutions they offer, with verification solutions dominating both groups of start-ups (>65%). It was also shown that most start-ups from the two groups have a multi-sectorial approach, although this approach is more pronounced for start-ups offering a more diversified product portfolio (45.5% compared to 40% of start-ups focusing on FR only). Another observation is that FR-only start-ups were found to have more retail or marketing products (35%) than start-ups with a broad portfolio, with retail representing 30.9% and marketing 29.1%. Moreover, the FR only group has less of a focus on transportation (20%), healthcare (18.3%), and finance (21.7%), whereas transportation alone is present in 30.9% of the uses of start-ups with a diversified product portfolio. Start-ups

offering a variety of products other than FR seem to propose sectorial uses for their products and the sector in which they could be implemented is often more precise than the group of FR-only start-ups, since the set of possible uses of the first group is more explicitly cited in public information than for start-ups focusing on FR only.

2.4. Business type

The study highlighted that the nature and variety of start-ups are dictated by their business model (Figure 8). For example, some tools are targeted directly at customers (i.e., individuals who will use facial recognition) while other tools are implemented by organisations for their own customers, as a part of their business activity. This distinction is particularly relevant when it comes to determining who is the controller of the processing being carried out, and therefore the recipient of the applicable law.

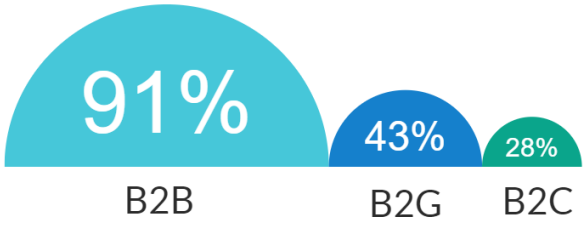

Figure 8. Business model type of start-ups
Note: n=126.

The analysis distinguishes between three business types:

- *B2B* (business-to-business) start-ups make commercial transactions with other businesses.
- *B2G* (business-to-government) start-ups offer solutions to public authorities.
- *B2C* (business-to-consumer) start-ups offer their products to individuals.

While start-ups dealing directly with the end customer (B2C) are in the minority (28%), it is important to note that these start-ups are the only data controller[6]. It is therefore their responsibility to comply with legal requirements. Conversely, start-ups that offer tools to companies (91%) or administrations (43%) are not necessarily exempt from being data controllers. However, they share the implementation of the legal obligations with the end-deployer. In these situations, it is important that the division of tasks is clearly expressed so that legal requirements apply to the relevant actors.

A more detailed analysis of the purposes for which FRTs are used in the context of the business model makes it possible to refine the legal issues, cases of use and deployment situations for these technologies. Although in most cases start-ups target the private sector, administrations and governments are also targeted, as well as individuals. The actual situation in which the system will be deployed may determine the different issues at stake, including legal issues.

Figure 9 presents an illustration of the situations in which FR technologies may be used by administrations and governments.

[6] For a definition of the concept of “data controller” see Section 3.3 below.

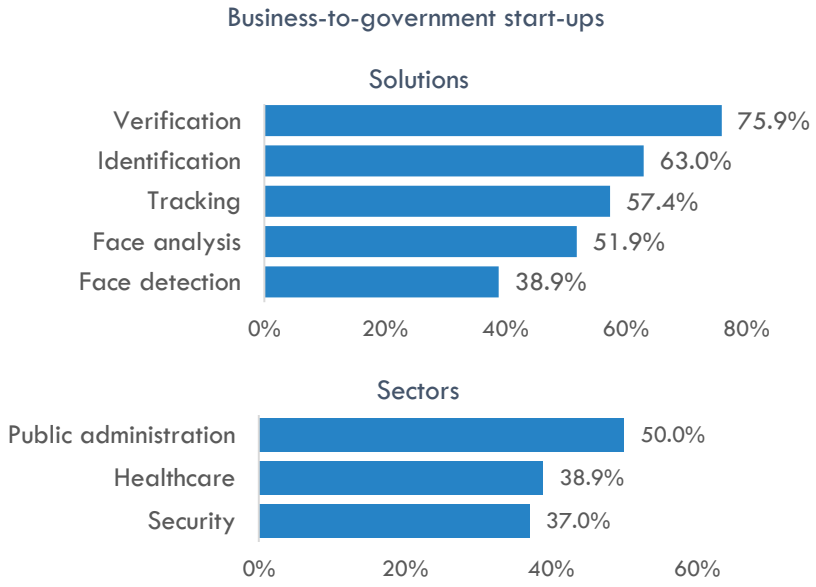

Figure 9. Solutions and sectors of B2G start-ups
Note: n=54.

Verification and identification purposes are predominant (75.9% and 63%, respectively) while face detection and face analysis technologies are less represented. Most of the time, FR devices are deployed or are intended to be deployed in public administration (50%) and some issues still require analysis such as the acceptance of these technologies by the workers[7], their adequacy, as well as a deeper analysis of these technologies' impact for the public sector[8] according to their use.

III. DATA PROTECTION APPROACHES OF FACIAL RECOGNITION START-UPS

This chapter presents an analysis of data protection approaches used by facial recognition start-ups based on their publicly accessible data. This includes the analysis of start-ups' efforts to present themselves as "privacy compliant", the documentation on data protection available on their websites**,** as well as the available information relative to their databases.

3.1. Efforts to show a privacy compliant public image

The public debate around facial recognition technologies and the various pieces of legislation that are being developed around the world[9] emphasise the need to adopt strong safeguards in order to protect privacy and respect data protection principles when using this technology[10].

[7] See for instance Ada Lovelace Institute Report, *Beyond face value: public attitudes to facial recognition technology*, 2019 ; European Union Agency for Fundamental Rights' (FRA) Report *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019.

[8] Similarly, a draft document prepared by Sub-Working Group 2 and presented to the Ad Hoc Committee on Artificial Intelligence (CAHAI) Policy Development Group (CAHAI-PDG) of the Council of Europe (CoE), *Artificial Intelligence in Public Sector*, on March 11, 2021, offers an analysis of the issues raised by algorithmic decisions in the public sector. It notably mentions computer vision such as "video or facial recognition to gain information on the external environment and/or the identity of specific person or objects" as one of the issues at stake.

[9] At the national level or through regional initiatives such as the proposed EU's AI Act.

[10] See for example the European Union Agency for Fundamental Rights' (FRA) Report *Facial recognition technology: fundamental rights considerations in the context of law enforcement* published in 2019 focused on the

Our study revealed that some start-ups are using their alleged compliance with the GDPR and respect for privacy in general as a marketing argument. Besides marketing considerations, several start-ups also put forward privacy considerations at the heart of their product's development.

FOCUS ON START-UPS

For instance, the Dutch start-up **20Face,** in its White Paper on *the future of access management: privacy-proof face recognition,* insists on "what the GDPR says about biometric data, how [to] ensure that [their] solution meets these requirements and how you can use facial recognition securely in your office building".

The start-up argues that the approach taken is not related to mass surveillance activities:

"[U]nlike police or other surveillance departments, 20faceNet is not simultaneously capturing images of and scooping up the image data of thousands or millions of other users who do not show explicit consent. By adaptively selecting the field-of-view of camera and recognition distance from camera to face, we photograph and process facial images of only those who have provided consent. By now it should have been clear that we do not compare a consumer's facial image to a database of facial images."

The study revealed that most of the time, when start-ups claim to be privacy compliant, it may be through general references to the General Data Protection Regulation (GDPR) or to other legislative texts regulating personal data, without necessarily providing further details on how compliance is ensured. Moreover, most of the analysed start-ups do not claim to be privacy compliant or, when they do, they only refer in general terms to legal texts currently in force (Figure 10).

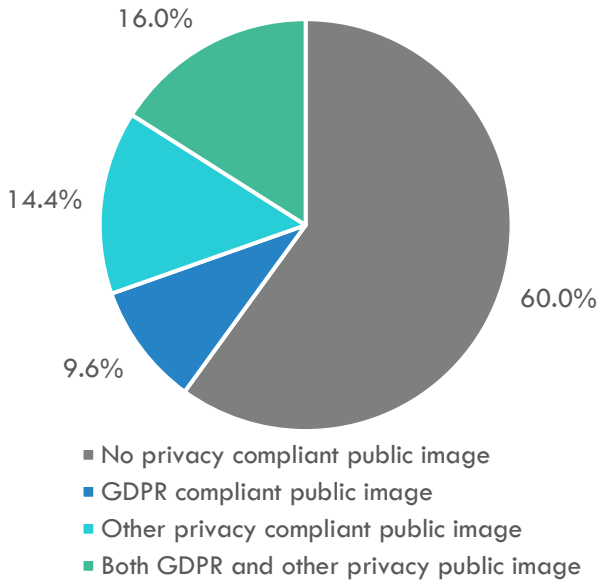

Figure 10. "Privacy compliant" public image of start-ups
Note: n=125.

use of FRTs for law enforcement and border-management purposes. Following this report, a civil society initiative *Reclaim your face* called for a ban on biometric mass surveillance in particular through the use of FRTs.

The study distinguishes between:

- Start-ups referring to the applicable *law(s)* without necessarily specifying which legislation is applicable to their technology.
- Start-ups specifying their position by mentioning the text(s) with which their technology is compliant. In this case, the *General Data Protection Regulation (GDPR)* is the main reference, which suggests the growing impact of the European framework in this field even outside of the European Union (EU)[11].

However, it should be noted that GDPR's influence extends beyond Europe (Figure 11).

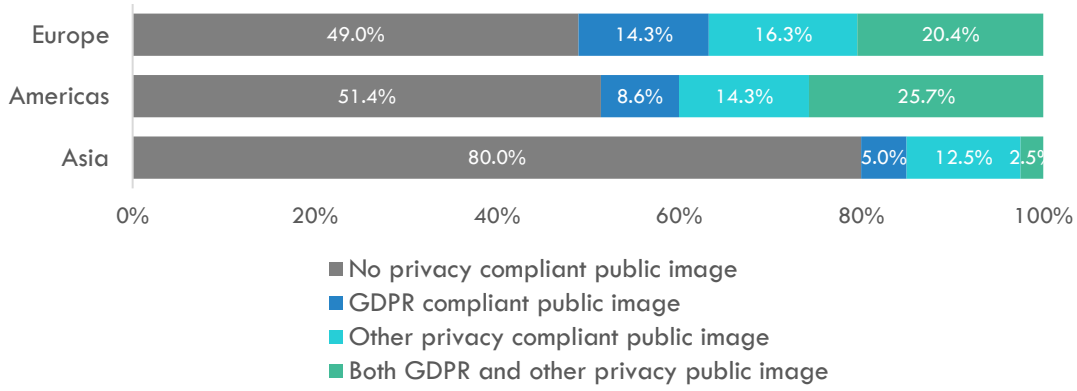

Figure 11. "Privacy compliant" public image of start-ups by continent
Note: Europe: n=49; Americas: n=35; Asia: n=40.

The results demonstrate that compliance with GDPR regulation is mostly mentioned by start-ups that have their headquarters located within the EU (35%). This observation is even stronger when analysing other privacy compliance mechanisms referred to by the start-ups (claims of privacy compliance for start-ups in Europe reach 51%). Accordingly, Europe is clearly one of the regions – along with the Americas – where claims of privacy compliance are most frequent.

FOCUS ON START-UPS

For instance, ubble.ai, a French start-up offering online identity verification solutions, detailed that their mission is to ensure trust and fight against fraud on the Internet, by enabling warehouses to verify the identity of users in a simple, reliable, secure and privacy-friendly way.

The start-up Smiley Owl Tech, a Spanish company developing products designed for cameras, demonstrates their public privacy compliant image, and notably their GDPR compliance, by highlighting having "received the European seal of Excellence by complying with all ethical standards".

Besides the EU, the Americas constitute the second region studied where GDPR is mentioned in claims of privacy compliance (34%). Whether it is to access the European market or to demonstrate a high level of standards in terms of privacy protection, several start-ups outside the EU are claiming that they adhere to the GDPR or to its values.

[11] For more information on the concept of the Brussels effect and the EU as a global actor in the field of digital regulation, see T. Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", 2020, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098.

FOCUS ON START-UPS

The Canadian start-up C2RO, designing products for robots, is a company that has a dedicated policy for their video analysis. Besides their vague mention of being “compliant with GDPR”, they specify that their system “has been deemed to not present high residual risks for the privacy rights of individuals". The start-up specifies that “[t]he Perceive™ architecture was audited and approved by Hass & Associates in Paris, France” and that they “have been recognized GDPR compliant by the CNIL, the national data protection authority in France, and have an approved Privacy Impact Assessment (PIA) from [their] DPO, allowing for large scale deployments of [their] solution across Europe”. Moreover, the start-up explains that “[they] have already deployed Perceive™ at various tier-1 customer and partner sites in Europe that have audited the system for compliance before the deployment".

Another start-up, Facenote, an American retail, image, and image-processing company offering live facial recognition (LFR) solutions to businesses and stores developed a “100% Opt-In”. The company details that they “value privacy over all. Customers decide to participate and be recognized by sending a selfie” but privacy comes “first” and “[a]s a user, you should decide where you want to be recognized, depending on the benefits, and what information you want to share".

Finally, Asia is a region where, although technologies deployment is rapidly increasing, claims of privacy compliance seem to be the least frequent (7,5% of references to GDPR and only 20% of start-ups mentioning a text or mechanism of compliance).

3.2. Accessible documentation on the data protection policy

In addition to the efforts made by start-ups to present themselves as “privacy compliant”, transparency is often a notion put forward to promote individuals’, investors’, and governments’ trust in these technologies and thus gain adherence. The study therefore looked at the documentation on data protection policies made available to the public by the start-ups (Figure 12).

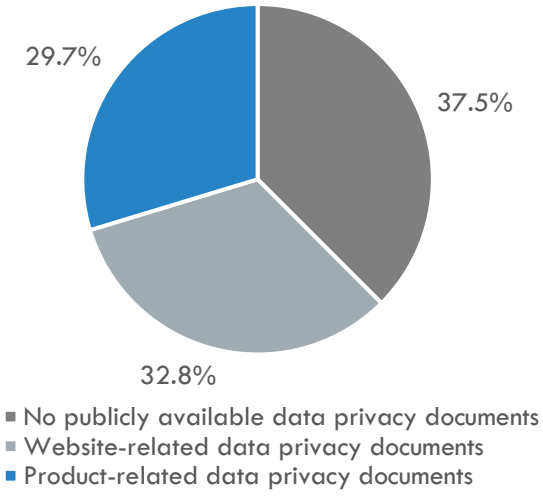

Figure 12. Publicly available data privacy documents of start-ups
Note: n=130. Website-related data privacy documents category includes start-ups with website-related data privacy documents only. Product-related data privacy documents category includes start-ups with product-related data privacy documents only and with both product- and website-related data privacy documents.

Users’ concerns about data protection are considered by the start-ups, most of which provide information on the subject (62.5%). Several start-ups also provide public documentation on how their products operate, outside of any prior contractual relationship. However, many of the

analysed start-ups (37.5%) do not make any documentation on their data protection policies available to the public.

- In most cases, when documentation is available, it is often related only to the protection of personal data that may be collected when visiting the start-up's *website* or when a visitor interacts with the start-up through contact forms (32.8% of start-ups). Furthermore, it should of course be emphasized that website related data privacy documents do not guarantee in and of themselves that the start-ups comply with data protection regulations.
- Results reveal that less than one third of start-ups (29.7%) actually make documentation publicly available to explain their data protection policies when it comes to the *use of their products and services* by their customers. This documentation is mainly found in the terms of use but can also be the subject of a separate document, which reinforces clarity. A more detailed analysis of the content of this documentation, when available, therefore seems interesting and we will proceed to it in the next section of this report.

A closer analysis of publicly available privacy documents by country is presented in Figure 13. Despite the existence of legal requirements in Europe on the provision of information relative to data protection information, publicly available data protection documentation was not found for a significant proportion of European start-ups[12].

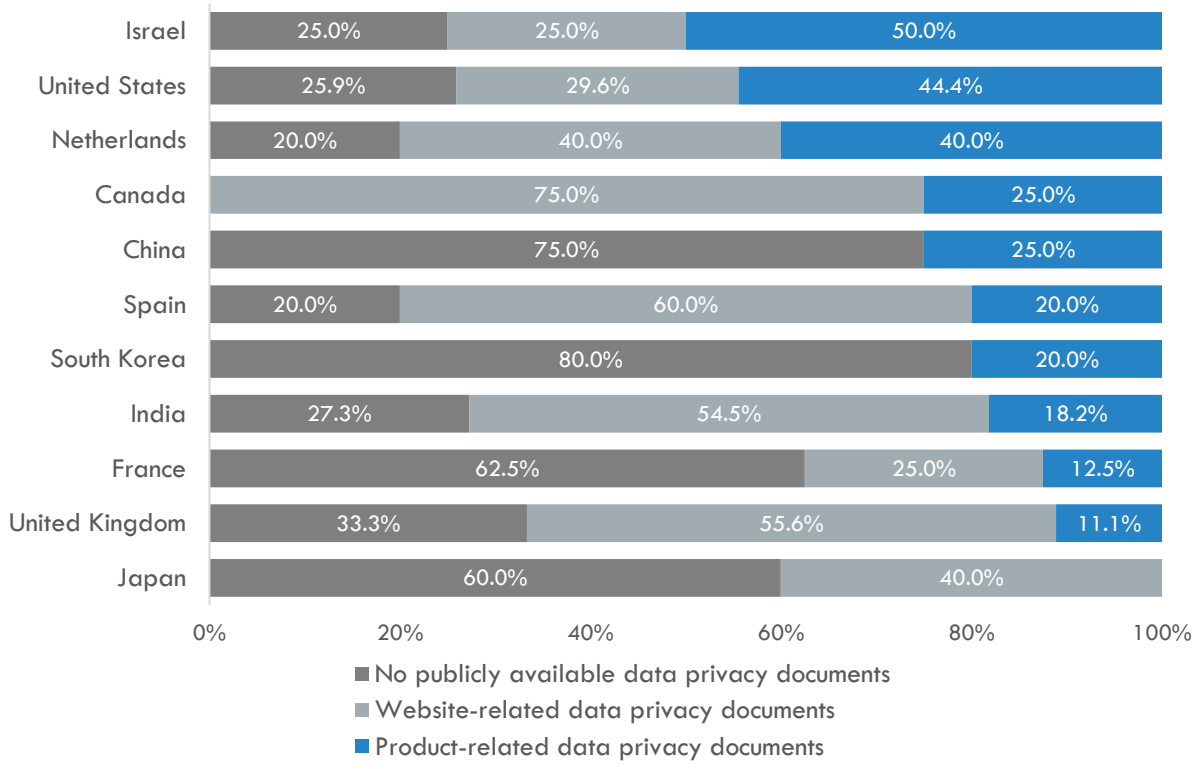

Figure 13. Publicly available data privacy documents of start-ups by country
Note: Israel: n=4; United States: n=27; Netherlands: n=5; Canada: n=4; China: n=4; Spain: n=5; South Korea: n=5; India: n=11; France: n=8; United Kingdom: n=9; Japan: n=5. Website-related data privacy documents category includes start-ups with website-related data privacy documents only. Product-related data privacy documents category includes start-ups with product-related data privacy documents only and with both product- and website-related data privacy documents.

[12] Note that the values displayed in Figure 13 are affected by the fact that the analysis included only start-ups with policies available in English or French languages.

3.3. Content of the data protection documentation

Data controller/ Data processor

Before discussing the content of the data protection policies implemented by the start-ups, it is useful to explain the notions and respective roles of the data controller and data processor. The data controller is responsible for ensuring that the processing carried out by the system complies with the legislation in force in case of any potential deployment[13]. The data processor is the one who actually does the data processing on behalf of the data controller, and must apply the legislation in its operations. To ensure full compliance with the current legislation, it is therefore necessary for each stakeholder involved to be aware of its obligations.

UNDERSTANDING: Data Controller/Data Processor

The GDPR defines these notions in Article 4:

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

The study of facial recognition start-ups highlighted the fact that the concepts of data controller and data processor are not widely addressed in their data protection documentation and potentially within their management system. In the framework of B2C, start-ups are generally both data controllers and data processors since there is no other intermediary between them and the end user. The distinction applies differently in the case of B2B and B2G start-ups. In these cases, the start-up might not deploy the technology directly; this operation can be performed by their client. However, there are cases when the start-up provides services related to the deployment of facial recognition, such as services related to the relevant database. In this context, the start-up may act as data processor on behalf of the client who is the data controller. Furthermore, start-ups may use the data generated by their clients to perfect their algorithms, which make them a data controller.

The study of the documents shows that these various issues related to the status of the data controller and/or data processor and the resulting distribution of obligations are most of the time not addressed in the documentation proposed and is not made publicly available by the start-ups. It might be desirable for such information to be incorporated into public documentation in order to determine the role of start-ups as data controllers/data processors once their products or services have been provided, and thus to specify the obligations incumbent on them.

[13] For more information see the Guidelines 07/2020 *on the concepts of controller and processor in the GDPR* adopted by the European Data Protection Board (EDPB) on September 2020.

FOCUS ON START-UPS

Though most of the start-ups do not publicly address their role as data controller in their public documentation, some start-ups' policy choices highlight their awareness regarding the sensitivity of the data that they are collecting and storing. The Italian start-up Cynny (MorphCast) offers an identification solution and an emotion recognition solution. According to their privacy policy, "Morphcast's emotional recognition AI does not record or archive any personal data" and "[a]ll images [are] deleted immediately" after the identification and no biometric data are stored on their server.

Common points

It is important to remember, as previously explained, that the number of start-ups providing publicly available data protection documentation on the use of their technologies is very limited. The following findings cannot therefore be extended and assumed to be valid for all the start-ups analysed. These are findings based on the 38 start-ups providing product-related data privacy documentation.
This being said, most start-ups that publish their data protection policies provide information on the same points:

- First, the *type of data* collected and, in particular, photos of individuals or facial templates. It is interesting to note that there is a difference between start-ups that claim to process biometric data, highlighting their sensitive nature and therefore the need for increased protection, and those that do not specifically define the data used.
- A second package often presents the *uses of the data* by a start-up as well as the *legal basis for this processing*. This is essentially the consent of the individuals but sometimes also the legitimate interest of the start-up.
- A third package of information relates to the *storage of data*. This includes information on anonymisation, storage security, and the length of time the data is to be kept.
- A fourth package of information is often related to the *transfer and disclosure of data*. This can be done to entities of three main types: the start-up's partners and subsidiaries, third-party economic actors and, finally, transfers required by law, particularly to the law enforcement authorities.
- Finally, a fifth and last package usually covers all the *rights of the individual* and the *means* of exercising them. Thus, the rights to access, rectification or objection are the rights most often explained.

3.4. Use of databases by start-ups

The use of facial recognition technologies in a broad sense does not necessarily entail the use of databases. However, databases can be used for identification, verification or tracking techniques. Indeed, when using verification techniques for granting access control to a building, for example, the comparison image can be stored centrally in a database and not on a separate support in the individual's possession (such as a biometric token). In tracking, where a face is tracked through different video sources, storage may be relevant, even if only temporarily. Whether databases are used impacts on a number of data protection issues. The storage of data also raises questions about data security and anonymisation. Finally, the issues of access to databases and the transfer of data are also crucial.

The analysis of start-ups showed that little information about the constitution of databases is publicly available. However, it was possible to identify a relatively important characteristic for some of them: the "location" of data storage (Figure 14).

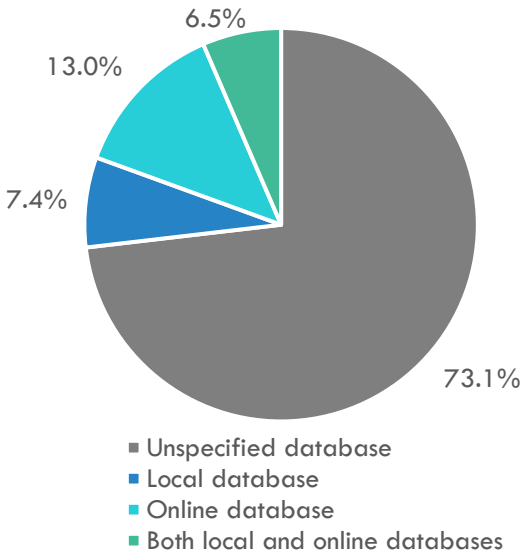

Figure 14. Databases of start-ups
Note: n=108.

- Some start-ups offer *local storage*, directly to a client, without the start-up necessarily having direct access to it.
- Conversely, other start-ups offer centralised, *online storage* of the databases relating to the operation of the proposed technology. In this case, a start-up has direct access to the data collected, which may be useful for its own activities. In such cases, the start-up can be considered as the data controller.

Finally, it should be noted that there is an almost systematic lack of information on the training of the various algorithms used in the context of facial analysis deployment, even though it is acknowledged that these databases play a significant role, particularly in terms of bias or the effectiveness of technologies.

FOCUS ON START-UPS

One of the exceptions to this observation is the Dutch start-up 20Face[14] which provided details in its White Paper about the ways its database was developed and on what basis. In fact, the start-up stated that the system was processing and storing facial images (photos) only of people who had given consent. Indeed, the start-up claims that "[u]nlike police or other surveillance departments, 20faceNet is not simultaneously capturing images of and scooping up the image data of thousands or millions of other users who do not show explicit consent".

As a comparison, the Russian start-up 3DiVi, affirmed in its online information that its system was comparing and matching features within a database of watchlists without providing further details on the origins of such databases, the type of categories of patents and their accuracy.

In the case of the American start-up Everalbum (later renamed Paravision), the American Federal Trade Commission (FTC) considered that the company deceived consumers about its use of facial recognition technology because it used customers' photos to develop facial recognition technology

[14] This start-up was previously analysed in the chapter III. 3.1 Efforts to show a privacy compliant image.

without telling them. The FTC issued a proposed settlement and ordered Everalbum to delete user data and any algorithms that had used this data.

A closer observation of start-ups with a local database (Figure 15) shows that most start-ups are B2B companies (93%). More than half of start-ups offer their solutions to government (60%), and 27% of start-ups provide products/services to individuals. In terms of sectors, the dominant applications include multi-sector, human resource management, transportation, finance, public administration, and smart city.

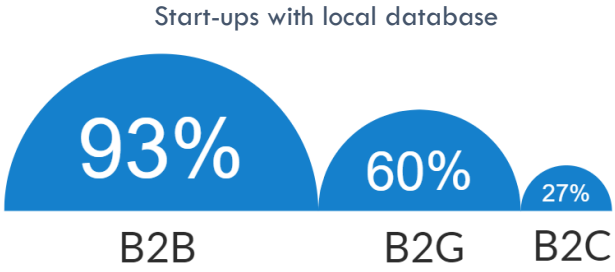

Figure 15. Start-ups with local database
Note: Includes start-ups with local database only and start-ups with both local and online databases. n=15.

IV. FACIAL RECOGNITION START-UPS IN THE CONTEXT OF THE COVID-19 PANDEMIC

This chapter focuses on how start-ups have strategically approached the Covid-19 pandemic. It also presents the various facial recognition tools and FR intended uses that have been developed by start-ups to help fight the pandemic.

4.1. Facial recognition and Covid-19

Since the end of 2019, States have been fighting the Covid-19 pandemic. Besides the unprecedented challenge that this pandemic has proven to be in terms of global public health, the pandemic has also been a technological challenge for start-ups developing their facial recognition systems as well as a regulatory challenge for States and organisations willing to promote these technologies while ensuring an adequate, ethical framework for them[15]. Governments had to quickly put in place measures to curb the pandemic such as compulsory wearing of masks, social distancing and other health measures, or contact-tracing apps.

Some start-ups developed their facial recognition technologies in order to help fight the pandemic. We found that 27 out of 130 start-ups studied (merely 20%) had developed and/or adapted their facial recognition technology to develop services to contribute to the fight against Covid-19. Some start-ups highlight the possibilities offered by FR technologies in this context on the main page of their website.

[15] See for instance the Council of Europe report "Digital solutions to fight COVID-19" which "analyses the impact on the rights to privacy and data protection of the measures taken to prevent the spread of the COVID-19 pandemic in the 55 African, Latin-American and European countries Parties to Convention 108".

The first prism of analysis was to investigate the reasons behind the choice of facial recognition technologies as a tool to fight the pandemic. First, facial recognition is a contactless technology, thus presented as particularly adapted to the fight against the transmission of Covid-19 given the conditions under which the virus spreads. Second, the video analysis features of this technology can allow authorities or companies to control whether measures to combat the pandemic are being applied. Start-ups proposed a wide range of monitoring tools, some of them – such as video analysis – able to quickly identify people wearing a mask or respecting social distancing or other measures.

The data studied here is not, however, sufficient to confirm that the Covid-19 crisis has been particularly favourable to the proliferation of facial recognition technology[16]. It is also interesting to note that none of the analysed start-ups were created specifically in response to the Covid-19 pandemic. Instead, already existing start-ups have shown that their technology could be or has already been adapted to meet the needs of the pandemic.

FOCUS ON START-UPS

For instance, the Russian start-up NTechlab (FindFace), which offers LFR solutions to governments and businesses[17], adapted its products to offer anti-Covid-19 solutions.

4.2. Types of utilisation

The analysis made it possible to highlight four main ways in which facial recognition technologies were used in the pandemic. These include mask detection to check that an individual is wearing the mask, facial recognition to verify identity of mask wearers even with a part of the face covered, identification and crowd management to check if there are too many people in the same place at the same time; and social distancing/interaction to check whether people are respecting the safety distances. If a start-up develops facial recognition technology capable of detecting faces, then it can also be used to detect people and therefore groups of people. Thus, start-ups can offer more varied uses such as detecting "risky" behaviours in the context of the pandemic (e.g., a person sneezing without a mask, detecting signs of illness, etc.) (Figure 16).

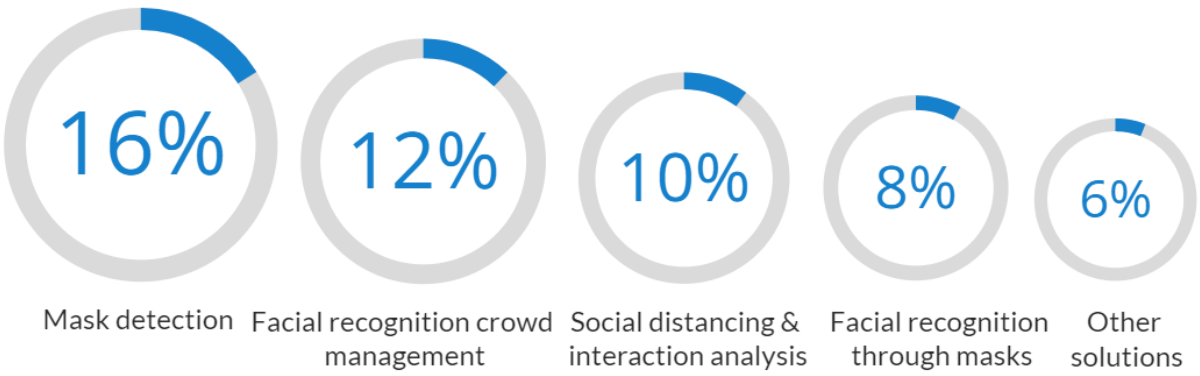

Figure 16. Solutions of facial recognition start-ups in the context of Covid-19
Note: n=130.

[16] See however Why Covid may mean more facial recognition tech by Chris Baraniuk, BBC news, 2020.
[17] See Remember FindFace? The Russian Facial Recognition Company just turned on a massive, Multimillion-Dollar Moscow Surveillance System, Thomas Brewster, Forbes 2020; Face recognition app taking Russia by storm may bring end to public anonymity, Shaun Walker, the Guardian, 2016.

The analysed start-ups were shown to offer the following FR solutions during the pandemic:

- *Mask detection*. The Covid-19 pandemic has led to a change in habits following the measures taken by governments. Facial recognition start-ups have found themselves facing a "technological challenge", that of scanning masked faces. In order to work, facial recognition must be able to scan the entire face, but the mask hides the lower part. As the mask has become an everyday object to be worn outdoors in multiple settings, start-ups have therefore adapted their products and added a mechanism to control the wearing of the mask.

FOCUS ON START-UPS

Datakalab is a French start-up founded by Frank Tapiro in 2016. While the start-up presents itself as "a French Technology company that develops computer image analysis algorithms to measure flows in public space"[18], it became famous during the Covid 19 pandemic thanks to its 'mask detection' solution. This mask detection tool was deployed at 'Châtelet les Halles' Paris subway station and in three markets of the City of Cannes. This system was intended to provide local authorities with a useful tool to implement their prevention measures to combat Covid 19. Xavier Fischer, Datakalab's CEO insisted on the fact that the mask detection solution they developed could not be assimilated to a facial recognition system since it does not enable individuals' identification and it is used only for statistical purposes[19].

The Spanish start-up Herta Security offers mask detection. It also offers individual identification even when people are wearing a mask.

UNDERSTANDING: What is object detection?

"Object detection is more interested in a class of object rather than a specific object such as an individual's face, by detecting instances of semantic objects of a certain class (such as humans, buildings, or cars) in digital images and videos. The goal of object detection is to detect all instances of objects from a known class, such as people, cars or faces in an image. This ability lends very well to such things as counting the number of cars in a carpark, people in a shop or even dwell time in an area without imposing on an individual's privacy".[20]

- *Facial recognition of mask wearers.* With the pandemic, one of the first measures adopted by governments was the compulsory wearing of a mask. Facial recognition algorithms use characteristic dots all over the face to identify a person. However, when wearing a mask, a large part of the face is covered, making identification more difficult. Despite this, some start-ups (8%) were able to adapt their facial recognition technology so that it can work even when the scanned individual's face is wearing a mask.

[18] See Datakalab official website, available at: https://www.datakalab.com/
[19] See REES (M.), « La CNIL se penche sur les caméras détectant le port du masque », Next inpact, Online, May 4th 2020, available at : https://www.nextinpact.com/article/30242/108956-la-cnil-se-penche-sur-camerasdetectant-port-masque
[20] Presence Orb, "Facial recognition vs Object recognition, are they different…Should you care?", January 7, 2020.

FOCUS ON START-UPS

For instance, the Canadian start-up Invixium offers innovative solutions, such as the IXM TITAN system, the most "cutting-edge processor ever created" incorporating touchless face recognition with or without masks, mask detection, and multifactor authentication.

UNDERSTANDING: How is facial recognition through the mask possible?

60 facial recognition configurations were evaluated to test the ability of AI systems to reliably collect and match images of individuals wearing an array of different face masks, in an event organised by the Science and Technology Directorate (S&T), which is the research and development unit within the US Department of Homeland Security (DHS) [21].
"On average, the different AI systems correctly identified 93% of unmasked individuals; for those wearing a mask, the identification rate reached an average of 77%.
The results, however, varied greatly from one system to the other: for example, the best-performing technology correctly identified individuals 96% of the time, even when they were wearing a mask. The worst-performing system tested during the rally, for its part, only identified 4% of masked individuals".[22]

- *Identification and crowd management.* The pandemic has led to the adoption of restrictive measures to limit the spread of the virus: stores, supermarkets, traders have had to manage the number of people returning to their establishments. Crowd management can be done manually, but start-ups have also adapted their object recognition systems to understand how many people are in a store and thus limit access when the entry threshold is reached.

FOCUS ON START-UPS

For instance, the Dutch start-up Sightcorp offers a technology capable of occupancy management and entrance flow management to thus comply with Covid-19 obligations.

- *Social distancing and interaction.* The ultimate measure that has been taken is social distancing which requires keeping a certain distance from each other and limiting interactions. Start-ups have also been able to respond to this demand by using their people detection and tracking tools to check whether people are respecting social distancing.

FOCUS ON START-UPS

For instance, the American start-up Paravision offers "wide-range solutions responding to the emerging needs created by the COVID-19 pandemic". It offers solutions in the workplace, airports, retail and beyond, through mask detection, face recognition with masks but also thermal detection and person detection and tracking. The latter allow their systems to be used for social distancing.

[21] See for instance the website of the US Department of Homeland Security – Biometric Technology Rally (2020)
[22] Daphne Leprince-Ringuet. D. "Facial recognition: Now algorithms can see through face masks", January 6, 2021.

- *Other uses.* Some start-ups go beyond the aforementioned utilisations, by promoting facial recognition and video analysis for less "conventional" purposes in the fight against Covid-19 like monitoring hand washing or detecting Covid-19 symptoms (see below)

FOCUS ON START-UPS

Here are several examples to illustrate these capabilities:

The Indian start-up Staqu Technologies, using its Jarvis technology, enables to follow and track daily hygiene activities such as hand washing, but also to monitor daily hygiene chores such as cleaning or sweeping, or to monitor and detect if there is an absence of safety equipment.

Another Indian start-up, Loksun Technologies, offers to “detect the symptoms of the disease”.

MoodMe, a start-up from Luxemburg, proposes to use augmented reality and the creation of filters in order to help public health campaigns by promoting safe behaviour and boosting morale.

V. CONCLUSION

There is an increasing interest in facial recognition technologies at the individual, business, and governmental levels. These technologies offer new opportunities to various industries and it is claimed that they could help increase safety and security, reduce direct human interaction, and make processes automatic, seamless, and more efficient. FRTs simultaneously raise a large number of legal and societal questions related to privacy, anonymity, violation of personal rights, data protection, data vulnerabilities, or unintentional biases in the algorithms. All these characteristics make FR technology and its applications a complex and controversial topic. This study aimed to provide new insights on the facial recognition uses and technologies by analysing FR start-ups from different countries. It notably investigated data protection approaches and documentation made publicly available by FR start-ups. Facial recognition tools were also examined in the context of the Covid-19 pandemic.

Consequently, the study allowed us to analyse the key functionalities, sectors, technologies, and business types related to start-ups developing facial recognition as well as the main countries developing these technologies. Furthermore, the report provides insights on the consideration by start-ups of the regulation of personal data, and their compliance with this regulation, or the efforts start-ups make to present themselves as being in compliance. In so doing, this report seeks to provide a better understanding of whether and how start-ups take into account the national provisions regulating personal data specific to their country, as well as the influence of the GDPR within the European Union and beyond.

The scope of this study was limited to 130 facial recognition start-ups worldwide. To qualify for selection, information about the start-ups’ technology and data protection documentation had to be available in English or French. Future studies could thus involve a larger sample of start-ups from different countries, as well as other types of companies, such as small and medium-sized enterprises (SMEs) or large organisations. Another limitation is related to the type of data collected, as this study analysed the textual data on start-ups’ websites and publicly available

documentation on the data protection policy. The results of this study could thus be complemented by a survey or interviews with firm founders/executives to collect additional information and get deeper insights on how data protection regulation is approached by the facial recognition start-ups.

Future research may also focus on the questions that some start-ups' activities raise in terms of human rights, fundamental rights as well as ethics. To use a particularly interesting example, the Israeli start-up Faception develops computer services that claim to be designed to reveal personalities and threats from peoples' face images in real-time. Faception professes to "offer[…] a breakthrough computer-vision and AI technology that analyses a person's facial image and automatically develops a personality profile, enabling security companies and agencies to more efficiently detect and apprehend potential offenders or criminals before they have the opportunity to do harm." The company further argues that their "algorithms can score an individual according to their fit" to certain classifiers, such as "people with high IQ", "white-collar offenders", "terrorists", or "paedophiles".

Future studies may also examine start-ups that have developed products and initiatives that enable, for example, medical advances to be made, such as the US start-up Brain Power, which develops glasses for interaction purposes and notably stimulates social and interaction skills in children with autism.

An update of the start-up landscape and further examination of these start-ups along the lines suggested above will enable a more precise analysis of the purposes of use and the conditions in which FR systems could raise significant legal and regulatory issues. Further studies are encouraged to continue the conversation with novel investigations and pathways at the intersection between facial recognition technologies and data protection regulation.

Annex I: List of 130 start-ups included in the study

Name[23]	Country	Year of creation	Website
20Face	Netherlands	2016	https://www.20face.com/en/
3DiVi	United States	2011	https://www.3divi.com/
3DUniversum	Netherlands	2014	https://3duniversum.com/
Adaptive Computation	United States	2011	https://adaptivecomputation.com/
Affectiva	United States	2009	https://www.affectiva.com/
Agrex.ai	India	2016	https://agrexai.com/
AIndra Labs	India	2016	https://www.aindralabs.com/
Alcatraz AI	United States	2016	https://www.alcatraz.ai/
Alchera	South Korea	2016	https://alcherainc.com/en/
AnyVision	Israel	2015	https://www.anyvision.co/
Astra Inc.	Taiwan	2016	https://www.astra.cloud/
Aurora AI	United Kingdom	1998	https://aurora-ai.com/
Authenteq	Iceland	2015	https://authenteq.com/
Bace	Ghana	2018	https://www.bacegroup.com/
Banuba	Belarus	2016	https://www.banuba.com/
Biometrypass	Chile	2012	http://www.biometrypass.com/
BLue Line Technology	United States	2013	https://bluelinetechnology.com/
BluePrintLab Inc.	South Korea	2014	https://www.blueprint-lab.com/
Brain Power	United States	2013	https://brain-power.com/
C2RO Robotics	Canada	2016	https://c2ro.com/
Cambridge Mechatronics Limited	United Kingdom	1995	https://www.cambridgemechatronics.com/en/
CaraCom	Finland	2017	https://www.caracom.fi/en/
Chooch	United States	2015	https://chooch.ai/
Clarifai	United States	2013	https://www.clarifai.com/
Clearview AI	United States	2017	https://clearview.ai/
Clofus	India	2016	https://clofus.com/
CloudWalk Technology	China	2015	https://www.cloudwalk.com/en/
Cognixion	United States	2014	https://www.cognixion.com/
Corsight AI	United States	2019	https://www.corsight.ai/
Datakalab	France	2016	https://www.datakalab.com/
D-ID	Israel	2017	https://www.deidentification.co/
DeepScore	Japan	2019	https://deepscore.ai/
Deepsense	France	2018	https://www.thedeepsense.co/
Digital Barriers	United Kingdom	2010	https://www.digitalbarriers.com/
Digitalattendant Co., Ltd.	Japan	2014	https://en.digitalattendant.co.jp/
EDGENeural.ai	India	2020	https://www.edgeneural.ai/
Electronic iDentification	Spain	2013	https://www.electronicid.eu/en

[23] The data were collected and the start-ups' websites were accessed and analysed between January and March 2021.

Emotics	Hong Kong	2017	https://www.emotics.co/
Erinfo	United States	2018	https://erinfo.me/
Eva Engines	France	2018	https://www.evaengines.com/
EyeAI	Ukraine	2018	https://eye-ai.tech/
Eyeverify (ZOLOZ)	United States	2017	http://eyeverify.com/
Faced.io (AReality3D Inc.)	United States	2012	https://faced.io/
FaceFirst	United States	2007	https://www.facefirst.com/
Facemap Infotechnologies	India	2012	https://www.facemap.in/
Facemetrics	Belarus	2018	https://facemetrics.io/
Facenote	Argentina	2016	https://facenote.me/
Faceout	Bermuda	2017	http://www.faceout.me/
FacePhi	Spain	2012	https://www.facephi.com/en/
Faception	Israel	2014	https://www.faception.com/
FaceX	India	2018	https://facex.io/
Fittingbox	France	2006	https://www.fittingbox.com/en/
Great Lite International Corp., Ltd.	Taiwan	2016	https://www.great-lite.com.tw/
GTRIIP	United States	2014	https://www.gtriip.com/
Hampentech	Hong Kong	2016	http://hampentech.com/
HB Innovation	South Korea	2013	http://www.hbinno.com/
Herta Security	Spain	2009	https://hertasecurity.com/
HiBrainy	France	2019	https://hibrainy.com/
Hyprsense	United States	2015	https://www.hyprsense.com/
I'm beside you	Japan	2020	https://www.imbesideyou.com/english
Innov Plus	France	2014	http://www.innov-plus.com/en/
Invision AI	Canada	2015	https://invision.ai/#Mission
Invixium	Canada	2012	https://www.invixium.com/
inVoid	India	2018	https://www.invoid.co/
iproov	United Kingdom	2011	https://www.iproov.com/
Jibo (NTT Disruption)	United States	2019	https://jibo.com/
Kairos AR	United States	2012	https://www.kairos.com/
Keocko	Hungary	2009	http://keocko.com/en/
KeyLemon SA	Switzerland	2008	https://www.keylemon.com/
LeapMind Inc	Japan	2012	https://leapmind.io/en/
Loksun Technologies	India	2018	https://loksun.ai/
LOQR	Portugal	2015	https://loqr.io
Meerkat	Brazil	2015	https://www.meerkat.com.br/
Megvii	China	2011	https://megvii.com/
MoodMe	Luxembourg	2015	https://www.mood-me.com/
Morphcast (Cynny)	Italy	2013	https://www.morphcast.com/
NTechLab	Russia	2015	https://ntechlab.com/
o.vision	Netherlands	2018	https://o.vision/
OneVisage	Switzerland	2013	https://www.onevisage.com/
Opsis	Singapore	2017	https://opsis.sg/

Orbo	India	2016	https://www.orbo.ai/
OrCam Technologies	Israel	2010	https://www.orcam.com/en/
Paravision	United States	2013	https://www.paravision.ai
Pixuate	India	2012	https://pixuate.com/
Plen Robotics	Japan	2017	https://plenrobotics.com/en/
Princeton Identity	United States	2016	https://princetonidentity.com/
PT Qlue Performa Indonesia	Indonesia	2016	https://www.qlue.co.id/
Pulchritudinous R&D	India	2019	https://www.prnd.xyz/
Raven	Canada	2015	https://ravenconnected.com/
RealEyes	United Kingdom	2007	https://www.realeyesit.com/
Reface	Ukraine	2018	https://reface.ai/
Reminiz	France	2014	www.reminiz.com/
Riddletag	Estonia	2019	https://riddletag.com/en/
Roborus	South Korea	2016	https://roborus.ai/
Saffe Payments	UK	2015	https://www.saffe.ai/
SeetaTech	China	2016	https://www.seetatech.com/
SeizeFace	United States	2016	https://www.seizeface.com/
Senscape Technologies	China	2010	https://www.senscape.com.cn/en/
SenseTime	Hong Kong	2014	https://www.sensetime.com/me-en
Sezame	Austria	2016	https://seza.me/
Sightcorp	Netherlands	2013	https://sightcorp.com/
Sighthound	United States	2013	https://www.sighthound.com/
SkyBiometry	Lithuania	2012	https://skybiometry.com/
Smiley Owl Tech S.L.	Spain	2012	https://smowl.net/en/
Staqu Technologies	India	2015	https://www.staqu.com/
Sumato-id	Argentina	2013	http://sumatoid.com/en/
Suprema	South Korea	2000	https://www.supremainc.com/en/
Tehnologii videoanaliza	Russia	2010	https://tevian.ru/
Trakomatic	Singapore	2013	https://www.trakomatic.com
Trueface.ai	United States	2013	https://www.trueface.ai
Trust Stamp	United States	2015	https://truststamp.ai/
Two-I	France	2017	https://two-i.com/
UAB Neurotechnology	Lithuania	1990	https://www.neurotechnology.com/
Ubble.ai	France	2018	https://www.ubble.ai/
Udentify	Turkey	2016	https://www.udentify.co/
Ugiat Technologies	Spain	2015	https://www.ugiat.com/
ULSee Inc.	Taiwan	2014	https://ulsee.com/#/
Uniqul	Finland	2013	https://uniqul.com/
Vedalabs	United States	2017	https://www.vedalabs.in/
VERONICA Technologies	Chile	2013	http://www.veronicacore.com/Home.aspx
Videmo	Germany	2008	https://videmo.de/en
Visio Ingenii	United Kingdom	2012	http://www.visioingenii.com/
VisionBox	Portugal	2001	https://www.vision-box.com/

VisionLabs	Netherlands	2012	https://visionlabs.ai/
Vook	Turkey	2017	https://www.vook.io/
WeSEE	United Kingdom	2016	https://www.wesee.com/
Wise AI	Malaysia	2018	https://wiseai.tech/
Yoti	United Kingdom	2014	https://www.yoti.com/
Zenus	United States	2015	https://www.zenus.ai/
Zirity	Estonia	2017	https://www.zirity.com/