SÉRGIO MIGUEL FERREIRA DOS SANTOS ABREU

LIVE FACIAL RECOGNITION TECHNOLOGIES IN EUROPEAN LAW – A DATA PROTECTION AND PRIVACY RIGHTS ASSESSMENT

Thesis submitted to obtain the

Master's degree in International and European Law

Coordinator:

Doctor Francisco Pereira Coutinho, Professor of the Nova School of Law

October 2020

PLAGIARISM DECLARATION

I hereby declare that the following dissertation and the ideas therein, are the result of my own study and research. No content has been copied or plagiarised from other authors' work. All materials used in its preparation have been duly referenced.

DECLARAÇÃO ANTIPLÁGIO

Declaro que a dissertação que se segue e as ideias que se apresentam são o resultado do meu próprio estudo e pesquisa. Nenhum conteúdo foi copiado ou plagiado do trabalho de outros autores. Todos os materiais usados na sua preparação estão devidamente referenciados.

NUMBER OF CHARACTERS

I declare that this dissertation's body, including spaces and footnotes, is composed of **153 283** characters.

NÚMERO DE CARACTERES

Declaro que o corpo desta dissertação, incluindo espaços e notas, ocupa um total de **153 283** caracteres.

INDEX

ABSTRACT

The following dissertation seeks to explore the deployment of live facial recognition technologies in the legal framework of the European Union, especially regarding the data protection and privacy rights of its citizens.

As we witness the dawn of what some are calling the "fourth industrial revolution", the deployment of artificial intelligence enabled technologies is no longer a farfetched futuristic horizon. Live facial recognition technologies, particularly, are already a reality in many European cities' landscapes, with various emerging pilot experiments, as will be shown throughout this dissertation.

While artificial intelligence is not a novelty *per se*, the pairing of machine learning with the explosive amounts of digital data (through which machines learn) being produced every minute, creates a fertile ground for artificial intelligence to blossom in. This leads to a plethora of possibilities to improve our day-to-day lives, but likewise increases the likelihood that the rights and freedoms of individuals are forsaken in the name of technological advances bolstered by economic and security interests.

In this context, live facial recognition technologies are steadily exerting pressure to permeate the European Union. It therefore becomes imperative to dissect the surrounding legal and political paradigm.

The end goal is to ascertain whether the European Union is ready to accommodate the brave new world of live facial recognition technologies. Towards that end, we will analyse some relevant decisions regarding the technology, not only in the European Union but also in transatlantic jurisdictions.

We will likewise be looking at how European Law is already capable of facing some of the challenges that arise from this technology and how it aims to further respond to the conundrums that will emanate from them. Along the way we will be offering some considerations on the virtues and defects of the journey towards the development and deployment of a technology that cannot subsist without data.

Keywords: Artificial Intelligence; Live Facial Recognition Technology; Personal Data; Privacy; European Law; Technological Regulation.

RESUMO

A dissertação que ora se apresenta procura explorar a implementação de tecnologias de reconhecimento facial no contexto legal da União Europeia, observadas através da lente da proteção de dados e direitos de privacidade dos seus cidadãos.

Enquanto testemunhamos aquilo que alguns autores têm referido como o despertar da "quarta revolução industrial", a implementação de tecnologias dotadas de inteligência artificial não está hoje num horizonte longínquo e rebuscado. As tecnologias de reconhecimento facial, particularmente, são já uma realidade no panorama de muitas cidades Europeias, contando com vários testes-piloto emergentes, como será demonstrado ao longo desta dissertação.

Embora a inteligência artificial não seja uma novidade, a combinação de *machine learning* com a quantidade explosiva de dados digitais hoje existentes (através dos quais as máquinas aprendem), potencia um solo fértil para que a inteligência artificial floresça. Tal resulta numa infinidade de possibilidades para melhorar o nosso dia-a-dia, mas de igual modo aumenta a possibilidade dos nossos direitos e liberdades serem ostracizados, em prol de avanços tecnológicos motivados por interesses económicos e de segurança.

Neste contexto, as tecnologias de reconhecimento facial têm exercido pressão para permear na União Europeia, pelo que se torna imperativo dissecar o contexto legal e político em que estas tecnologias se inserem.

Assim, esta dissertação pretende observar a aptidão da União Europeia para acomodar o admirável mundo novo das tecnologias de reconhecimento facial. Para

este fim, iremos analisar algumas das decisões relevantes referentes a esta tecnologia, emanadas não só dentro da União Europeia, mas também de jurisdições transatlânticas.

Iremos de igual modo observar como o Direito da União Europeia é já capaz de fazer face a alguns dos desafios que brotam desta tecnologia, mas também como ele poderá vir a responder a alguns dos dilemas que dela emanarão. Pelo caminho serão também tecidas algumas considerações sobre as virtudes e defeitos dessa jornada, com vista ao desenvolvimento e implementação duma tecnologia que não poderá subsistir sem dados.

Palavras-Chave: Inteligência Artificial; Tecnologia de Reconhecimento Facial; Dados Pessoais; Privacidade; Direito da União Europeia; Regulação tecnológica.

ABBREVIATIONS

AI – Artificial Intelligence

AI HLEG – Artificial Intelligence High-Level Expert Group

B2B – Business to Business

B2C – Business to Consumer

CCTV – Closed-Circuit Television

Charter – Charter of Fundamental Rights of the European Union

CJEU – Court of Justice of the European Union

DPA – Data Protection Authority

EC – European Commission

ECHR – European Convention on Human Rights

ECtHR – European Court of Human Rights

EDPB – European Data Protection Board

EU – European Union

FRTs – Facial Recognition Technologies

GDPR – General Data Protection Regulation

LFRTs – Live Facial Recognition Technologies

ML – Machine learning

UAV – Unmanned Aerial Vehicle

UDHR – Universal Declaration of Human Rights

XAI – Explainable Artificial Intelligence

I – INTRODUCTION

In 1949, George Orwell's novel "1984" [1] made reference to a metallic object known as the "telescreen", which scrutinized every movement of the citizens of a dystopic society engulfed in mass surveillance. In a work that delves into a technology which goes hand in hand with Orwellian fiction, mentioning the literature classic might be somewhat of a *cliché*. However, if we take a glance at China's "automated authoritarianism" and its construction of "virtual cages"[2] through the aid of live facial recognition technologies (LFRTs) – which is especially notable regarding the control of the Uighur and other ethnic minorities in the Xinjiang area of China – it becomes hard not to draw parallels between fiction and reality.

Indeed, the "Social Credit Score" system that Jack Ma's enterprise Alibaba has developed and implemented in China is akin to a dystopic scenario. As an example, a blacklisted person (someone who has received a certain number of negative "social reviews") will be named and shamed, in the most mundane situations. As written in a Time magazine's article from 2019, when "a blacklisted person crosses certain intersections in Beijing, facial-recognition technology projects their face and ID number on massive electronic billboards" [3].

What one can take from the work-of-fiction's cautionary tale is that these tools, in the hands of an authoritarian government, can prove to be a devastating blow to fundamental rights and freedoms.

[1] ORWELL, George. "1984", Penguin Books, London, (first published in 1949), 2008.
[2] BUCKLEY, Chris; MOZUR, Paul; RAMZY, Austin. How China turned a city into a prison: A surveillance state reaches new heights. The New York Times, [online] 2019, Available at: <https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html> [Accessed 25 September 2020].
[3] CAMPBELL, Charlie. How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens. time. com/collection/davos-2019/5502592/china-social-credit-score, [online] 2019, Available at: <https://time.com/collection/davos-2019/5502592/china-social-credit-score/> [Accessed 25 September 2020].

The case of China and its ever-expanding arm, encroaching into the personal lives of its citizens is however not an exclusivity of the East. The West has evidently joined in on the AI race and facial recognition has followed suit.

As we delve deeper into this topic, some notable cases – though the jurisprudence is not yet abundant – will be brought to the forefront of the discussion. We will be looking mainly at the European reality, but also at the Northern and Southern American take on this topic.

As of this date, the European Commission has released a white paper[4] on Artificial Intelligence, as part of Ursula von der Leyen's plan to create a "Europe fit for the digital age". This paper and the work that surrounded it will be promptly dissected, as to aid us on understanding what is the current political stance regarding AI and in particular the technology this dissertation aims to focus on.

After exploring the political paradigm surrounding our topic, we will move on to the analysis of primary and secondary law that will be called upon to regulate the technology of facial recognition. We will be aiming to showcase how this legislation may already 'accommodate' this technology, while underscoring some of the grey legislative areas.

1 – LFRTs in the public and private sector

To further add on this introductory note, it should be made clear that this work will not act as a paladin crusading for the demonization of LFRTs. Undoubtedly, under a clear and strong legal framework, these technologies may find a place in our society and be a most welcome gift of innovation to better our lives, especially improving law enforcement authorities' means to deter crime.

This brings us to one of the biggest arguments in favour of LFRTs – crime prevention. This overlapping relationship between these technologies and the

[4] 2020. WHITE PAPER on Artificial Intelligence - A European Approach To Excellence And Trust. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [Accessed 25 September 2020].

claims for state defence and security are not new. Take the notable example of what happened after the terrorist attacks of September 2001, when many turned to technology questioning whether such attacks could have been prevented, had there been the right technological tools at the airport security checks where the terrorists embarked. This phenomenon, which has been called by Pat Gill as "technostalgia"[5], is a "desire to revise the past to redetermine the present by harnessing technology toward human ends, all the while recognizing the impossibility of the endeavour"[6].

Almost 20 years have passed, and the nostalgia for a technology that is not existent or practical has been replaced by a paradigm where such technology is not only practical but can be found quite literally at the end of our fingertips, with many of the most recent smartphones having the feature of unlocking through facial recognition.

The technological developments of recent years and the massive amounts of data being produced every second, combined with rising geopolitical tensions and terrorist movements, explain why the EU must be wary of the politization of such technologies amidst its Member-States. In a time where Europe is seeing the rise of new demagogues who see fear as their trojan horse to infiltrate politics, it is fathomable that such tools, under a weak or grey legislative area, can be harnessed in the name of security, and later be repurposed towards authoritarian ends. Alas, it is important to recall that even non-authoritarian states can become one if the (in)correct jigsaw pieces fall into place, for "power tends to corrupt, and absolute power corrupts absolutely"[7].

But not only the public sphere can benefit from facial recognition technologies. While LFRTs gained traction, notably on a "smart" surveillance level, pushed by

[5] GILL, Pat. Technostalgia: Making the future past perfect. Camera Obscura: Feminism, Culture, and Media Studies, 1997.
[6] GATES, Kelly A. Our biometric future: Facial recognition technology and the culture of surveillance. NYU Press, 2011, p.2.
[7] ACTON, Lord. Letter to Bishop Mandell Creighton. Retrieved on June, 1887, 29, 2009.

defence and security social actors (e.g. the military or law enforcement agents)[8], they are likewise relevant on a marketing level, as it is expected that the facial recognition market grows from $4 billion in 2017 to anywhere between $7.7[9] or 9.2[10] billion in 2022.

Truthfully, LFRTs are very valuable to marketeers, for example, by analysing the facial expressions of a consumer when confronted with an advertisement[11] or by monitoring individuals' shopping preferences when on a mall. They can likewise be useful to scan crowds at private venues such as music festivals or football stadiums[12] in search of banned persons, or even check a student's attendance in school.

Both the public and private sector's usage of LFRTs is going to be analysed during this dissertation. The focus will however be placed in the public sector, notably law enforcement's usage of the technology, as such is the area that can lead to the direst violations of rights and freedoms of individuals.

2 – Definitions

Before delving deeper into the aspects surrounding the topic of LFRTs, it is important to provide the reader with some initial definitions and a somewhat simplistic view of the technical aspects underlying such technology. This is not meant to be an exhaustive approach to these definitions as they will come into play

[8] GATES, Kelly A. Our biometric future: Facial recognition technology and the culture of surveillance. NYU Press, 2011, p.3.

[9] Norton, 2020. How Does Facial Recognition Work? [online] Available at: <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> [Accessed 25 September 2020].

[10] MARR, Bernard, 2019, Facial Recognition Technology: Here Are the Important Pros And Cons. Forbes [online]. 2019. Available from: <https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#61deecf714d1> [Accessed 25 September 2020].

[11] DEMARTINI, Felipe, 2018. Justiça Ordena Fim De Coleta De Dados Faciais Na Linha Amarela Do Metrô De SP. [online] Canaltech. Available at: <https://canaltech.com.br/seguranca/justica-ordena-fim-de-coleta-de-dados-faciais-na-linha-amarela-do-metro-de-sp-122744/> [Accessed 25 September 2020].

[12] EDRi. 2019. Danish DPA Approves Automated Facial Recognition. [online] Available at: <https://edri.org/danish-dpa-approves-automated-facial-recognition/> [Accessed 25 September 2020].

later in this dissertation, however a preliminary explanation is an essential roadmap for the path ahead.

2.1 – Personal data and Biometric Data

Taking a direct quote from article 4, (1) of the General Data Protection Regulation (EU) 2016/679, personal data is "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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, generic, mental, economic, cultural or social identity of that natural person".

Amongst personal data we can find, specifically, biometric data, which will be the pivotal data to be considered on a dissertation of this nature. Once more, we can obtain a thorough definition from the GDPR's article 4, (14) wherein it is asserted that biometric data is "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 (…)".

Biometric data corresponds to a special category of personal data under the GDPR, for this reason, the processing of biometric data must comply with stricter criteria. In principle, the processing of such data categories is prohibited, unless one of the exceptions listed in article 9 of that legislation applies. In due course we will approach this and other articles of the GDPR in more detail.

Notwithstanding the aforementioned, it should be noted that "[t]he processing of photographs should not systemically 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" (Recital 51 of the GDPR). What this means is that the processing of photographs will only be considered under article 9, if such processing happens to allow identification or authentication of the person concerned. In any case, it is not easy to grasp a usage of LFRTs that could escape this definition.

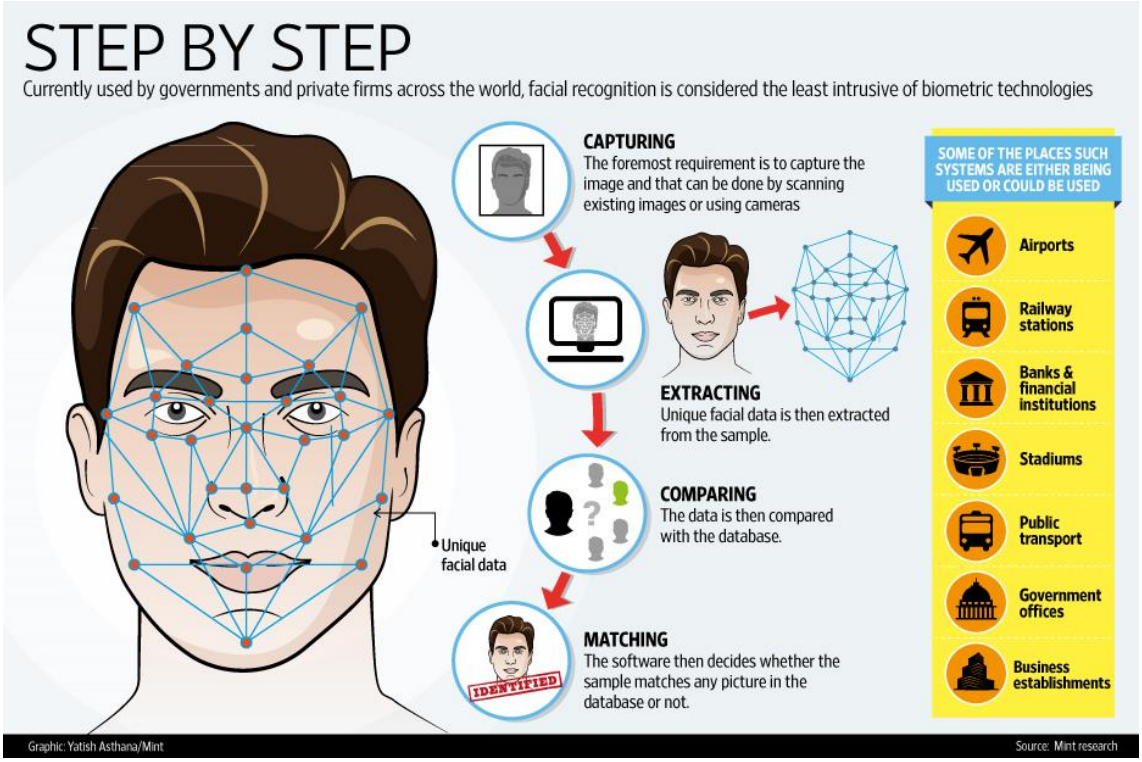
2.2 – Live Facial Recognition Technologies

LFRTs rely on biometric data, a special category of personal data, to automatically identify[13] human faces and/or recognise facial expressions, by matching these with photographs stored in a database. Firstly, a face is identified from a live camera feed; secondly, the software analyses the geometry of the face (e.g. distance between the eyes; width of the mouth; length of the nose; etc.) – these facial features are called nodal points[14] and when combined result in a faceprint or facial signature translated into a mathematical formula; fourthly, the software crosschecks the facial signature with a database to find a match of the picture taken[15] – this database is commonly called a "watchlist", which can consist of pictures of persons of interest (PoI), wanted criminals, missing children, *et cetera*.

[13] It should be noted that in facial recognition systems, identification is not the same as authentication or verification, the latter relates to the comparison of two biometric templates – one-to-one matching - which in principle belong to the same individual, this is the procedure used at Automated Border Control (ABC) in airports. The former, checks the biometric data against a large database.

[14] RAO, Varuna. Face Recognition: Is It a Match? Oklahoma Academy of Science Publication, 2009, p. 3.

[15] Norton, 2020. How Does Facial Recognition Work? [online] Available at: <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> [Accessed 25 September 2020].



Graph by Yatish Ashtana/Mint; Source: Mint research

It is relevant to make the distinction between the more common and standard facial recognition technology software and the more recent *live* facial recognition technology. The first refers to a technology that can function offline (e.g. uploading a facial image of an unidentified citizen to a software which scans a database for a possible match); LFRT refers to live camera footage being analysed on the fly, with the software dynamically collecting and processing new data and crosschecking it with a database to find a possible match.

This is an especially important distinction, as LFRTs have the potential of being either a software that scans crowds for specific persons of interest present on a database, or a technology that can be used to extract facial features from people at large, irrespective of their presence on a database or not, adding them to a watchlist, for no particular reason other than for mass surveillance purposes.

2.3 – Artificial Intelligence

The technology we have previously mentioned is enabled by the existence of artificial intelligence (AI).

AI is a subpart of computer science, which seeks "to give computers the sophistication to act intelligently"[16] or propose decisions. It "refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (…) or AI can be embedded in hardware devices."[17]

In short, AI is present in our daily lives, be it when an email is detected as spam, when a product is recommended to us through an ad based on our search history, or when a software automatically matches the facial features of a person to a facial image stored in a database.

2.4 – Machine Learning

This revolution of AI can be credited to Machine Learning (ML). Instead of programming the software to reply X if Y is true, ML is a set of algorithms that allow a machine or software to train its artificial intelligence through the data provided to it. An example of ML can be seen when we input series or movies we like in a streaming service and receive as output series or movie recommendations.

On the domain of LFRTs, the software can be given an image of two similar persons and be asked to identify who the face belongs to (crosschecking the input with previous images stored in a database). Once the software provides an output, it is followed by a human adjudication that selects whether the software was right

[16] NILSSON, Nils J., Principles of artificial intelligence. Morgan Kaufmann, 2014, p.1.
[17] EUROPEAN COMMISSION. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final, p. 2.

or wrong. This human input will be registered, allowing the computer to learn from its own mistakes.

Furthermore, there are even more complex sets of algorithms such as deep learning or reinforcement learning that have further entrenched the development of functioning AI within our daily lives. However, for the sake of simplicity, we will not delve deeper into these concepts.

2.5 – Databases

As stated, LFRTs rely on the existence of databases which are composed of individuals' biometric data. What many people will not be aware of is that there is a high chance that their facial images are already stored in some databases.

Take the example of recent smartphones – if users wish to unlock their phones faster, through technologies like "Face ID" on the Apple's iPhone, all they need to do is provide their facial features.

Unsurprisingly, Google, Facebook, Instagram and most social medias also have databases, which we – as users – willingly contribute to, by uploading our facial features or the facial features of friends, who we then 'tag' as to identify them. This allows for an easier training of facial recognition algorithms as there is a bigger and more diverse dataset to analyse through machine learning (specifically deep learning). This explains why, amidst Facebook, a research group called "Deepface" was created, which has achieved facial recognition technology with an accuracy of 97.35%[18].

a) Clearview AI

Perhaps more worryingly, from a personal data protection perspective, earlier in 2020, "Clearview AI", a US start-up company, launched a revolutionary facial

[18] TAIGMAN, Yaniv, et al. Deepface: Closing the gap to human-level performance in face verification. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2014. p. 1701-1708, p. 7.

recognition app, that draws its database from over 3 billion photos scraped from social media such as Facebook, YouTube or Venmo. According to the Company's founder Hoan Ton-That, "Clearview is basically a search engine for faces"[19] that anyone in law enforcement can use by uploading a face to the system which finds any other publicly available material and matches that particular face. The founder of the controversial company further stated that over 600 law enforcement agencies have begun to use the platform in 2019.

Despite claims that the technology was "strictly for law enforcement", recent leaks have shown that Clearview AI has been used by private firms such as Walmart or Macy's, which can use the software to run background checks on potential employees[20].

In this context, the European Commission (EC) has consulted EU data protection authorities, as it is rumoured that the start-up might be trying to expand overseas to countries such as Italy, Greece and the Netherlands[21]. Moreover, a recent Swedish DPA inquiry has revealed that the technology is indeed already being used in the country by law enforcement[22].

In June of the current year, the EC made clear in the European Parliament (EP) that it was not aware of the 'face recognition software' application being used in Europe, but warned that if such was the case, the technology would have to comply with EU data protection rules, specifically article 9(1) of the GDPR, which

[19] O'SULLIVAN, Donnie. This man says he's stockpiling billions of our photos'. CNN Business, February 2020, 10. Available at: < https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html> [Accessed 25 September 2020].
[20] WOOD, Charlie, 2020. Leaked Documents Reportedly Show Clearview AI Tech Was Used by Walmart And Many Private Firms — Contradicting Its Claims It Only Works with Law Enforcement. [online] Business Insider. Available at: <https://www.businessinsider.com/clearview-ai-reportedly-sold-tech-to-fbi-other-enfocrement-agencies-2020-2> [Accessed 25September 2020].
[21] STOLTON, Samuel, 2020. After Clearview AI Scandal, Commission 'In Close Contact' With EU Data Authorities. [online] www.euractiv.com. Available at: <https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/> [Accessed 25 September 2020].
[22] MANANCOURT, Vincent, 2020. Controversial US Facial Recognition Technology Likely Illegal, EU Body Says. [online] POLITICO. Available at: <https://www.politico.eu/article/clearview-ai-use-likely-illegal-says-eu-data-protection-watchdog/> [Accessed 25 September 2020].

prohibits the processing of biometric data for the purpose of uniquely identifying a natural person[23].

The aforementioned sheds light on the fact that LFRTs can pose dangers to individual freedoms and rights from their inception. The same is to say that LFRTs' databases and the datasets therein might be obtained with disregard towards ethical or legal considerations. This prompts us to discuss the technology through an ethical and legal lens, understanding the importance of privacy and data protection, and how mass surveillance can be prejudicial towards human development. It follows that an ethical approach is exactly the *modus operandi* the EU seems to be opting for, as will be explored further on. Under this impetus, our next chapter will be devoted to the right to privacy and the ethics behind facial recognitions technologies.

[23] Ylva Johansson. Answer given on behalf of the European Commission regarding Parliamentary questions on the 3rd of June 2020. Europarl.europa.eu. 2020. Answer for Question E-000383/20. [online] Available at: <https://www.europarl.europa.eu/doceo/document/E-9-2020-000383-ASW_EN.html> [Accessed 25 September 2020].

II – LFRTs AND PRIVACY - THE CASE FOR THE "RIGHT TO OBSCURITY"

In 1890, Louis Brandeis and Samuel Warren wrote in the Harvard Law review the following paragraph:

"*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops*."[24]

Though over a century old and referring to the breach of privacy made by the invention of instant photography, the quoted article still translates easily to today's paradigm and makes a fine case for the right to privacy – a "right to be let alone".

Fast forward to 2020 and we find ourselves in a reality in which privacy seems to have shapeshifted and diluted itself with what is public. A quick browse through someone's social media page will suffice to offer us a doorway into a stranger's life; a plethora of apps collect our personal data in exchange for an easier undertaking of the most mundane tasks – all we need to do is accept the (in)famous terms and conditions. This narrowing of the private sphere, this willingness to open our intimate lives to reap the rewards of technology can contribute to the acceptance of LFRTs without the necessary considerations regarding their impacts on the freedom of the individual.

It is amidst this apparent difficulty of separating the public and private that the word "obscurity" has begun to be used regarding privacy law. In this context,

[24] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, 1890, p. 195.

"[o]bscurity is the idea that when information is hard to obtain or understand, it is, to some degree, safe."[25]

Quoting the American Federal Trade Commissioner Julie Brill, "[o]bscurity means that personal information isn't readily available to just anyone. It doesn't mean that information is wiped out or even locked up; rather, it means that some combination of factors makes certain types of information relatively hard to find."[26]

An example of personal obscurity-seeking can be through the usage of websites that do not show up on standard search engines; the usage of online pseudonyms; VPNs; or using a mask in public, to hide some facial features as to not be recognised by LFRTs.

Regarding this last example, it is worth mentioning that the British Met Police has completed ten trials of LFRTs in London, deploying the technology in "Facial Recognition Zones"[27]. In February of the current year, in one of those trials, a man who did not want to have his face scanned passing by an area where the technology was set-up, decided to cover his face. He was approached and stopped by the Police who demanded that the man uncovered his face and then proceeded to photograph him against his will.[28]

It is worth inquiring on the legitimacy of decisions of this nature, which we can only estimate will become more common in the future.

[25] HARTZOG, Woodrow; SELINGER, Evan. Surveillance as loss of obscurity. Wash. & Lee L. Rev., 2015, 72, p. 1358.
[26] SELINGER, Evan; HARTZOG, Woodrow. Why you have the right to obscurity. Christian Science Monitor (Apr. 15, 2015), 2015.
[27] Met.police.uk. n.d. Update on Facial Recognition. [online] Available at: <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/> [Accessed 25 September 2020].
[28] Fines and Facial Recognition - BBC Click. 2019. [video] London, U.K.: BBC. Available at: <https://www.youtube.com/watch?v=0oJqJkfTdAg/> [Accessed 25 September 2020].

Moreover, it is important to understand that not everything that happens in the public sphere should be public knowledge. The following example given by Solove[29] clearly illustrates this:

"(…) A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities. (…)"

The illation we can draw from the aforementioned citation is that public spaces are not necessarily a barren land of privacy, and that individuals can rely on a right to maintain some obscurity.

In *Peck v. the United Kingdom*[30], a similar stance was taken by the European Court of Human Rights (ECtHR). In that case, the Court unsurprisingly found that the disclosure to the public of video surveillance which depicted a man attempting suicide in a public place, was a "disproportionate and therefore unjustified interference with his private life and a violation of article 8 of the [European Convention on Human Rights]" (paragraph 87).

It is worth underscoring that the same court considered photographs – an essential piece on the facial recognition puzzle (as videos are in essence multiple photographs taken in rapid succession) – as "one of the chief attributes of (…) personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers"[31].

Notwithstanding, in the aforementioned case of Peck, the UK's Government contended that there had been no interference with the right to private life of the applicant, as the incident had happened on a public location, which rendered the actions of the applicant as part of the public domain (par. 53).

[29] SOLOVE, Daniel, The digital person: Technology and privacy in the information age. NyU Press, 2004, p. 44.
[30] ECtHR, Case of Peck v. the United Kingdom, 2003.
[31] ECtHR, Case of López Ribalda and Others v. Spain, 2019, paragraph 89.

The applicant countered by asserting he was not aware he was being filmed and that the disclosure of the images to millions of people, amongst which his family and friends, had been a dire violation on his right to private life (par. 54).

Moreover, he claimed he had been on the street late at night, that he was not taking part in a public demonstration and, given his psychological state, it could not be said that he was voluntarily at the filmed location (par. 55).

The Court's assessment regarding this point was that while "CCTV cameras in public places play an important role in both crime prevention and crime detection" (par. 32) even on public spaces, to a certain extent, there is bound to exist a reasonable expectation of privacy (pars. 58 and 59).

This brief jurisprudential analysis points us to the fact that the right to obscurity, as a corollary of the right to privacy, becomes increasingly important in a paradigm where technology is increasingly breaching our intimate, which necessarily needs to be fortressed. The existence of a right to obscurity is a pre-requisite to a safe haven, a place of refuge for the individual – a mitigation of the damages a surveillance society may pose. Ultimately, it is the realization that "[j]ust because we have sleepwalked into a surveillance society doesn't mean we should refuse to wake up"[32].

The thesis of Selinger and Hartzog, which claims that obscurity should be at the center of the surveillance debate[33], should not be dismissed when considering the implementation of LFRTs in the EU and the implications on the rights to privacy of EU citizens.

[32] LAZAR, Seth, BENN, Claire and GÜNTHER, Mario, 2020, Large-scale facial recognition is incompatible with a free society. The Conversation [online]. 2020. Available from: https://theconversation.com/large-scale-facial-recognition-is-incompatible-with-a-free-society-126282 [Accessed 25 September 2020].

[33] HARTZOG, Woodrow; SELINGER, Evan. Surveillance as loss of obscurity. Wash. & Lee L. Rev., 2015, 72, p. 1346.

As evidenced through the case law above, the right to obscurity is not a newfound legal paradigm that will hardly be adaptable to technologies such as LFRTs. It is a concept that is already in motion in the EU legal context, even if camouflaged under different legal linguistics. For this reason, one might expect (and hope) that the right to obscurity is already implicit amidst legislation which enshrines the right to privacy of European citizens (e.g. the Charter of Fundamental Rights of the European Union).

But this is also true regarding data protection legislation, in this context, it is important to recall a landmark case of the Court of Justice of the European Union (the Court of Justice), the Google Spain v. AEPD[34]. This case resulted in the so-called "right to be forgotten" – which gained legal recognition in article 17 of the General Data Protection Regulation (GDPR).

As some authors have argued, the caveat should be made that more so than a "right to be forgotten", the case of Costeja González, presented a "right to preserve obscurity"[35]. Moreover, some believe that "(…) [t]he rulings do not even include any reference to the concept of "forgetting". Instead, the court creates a limited ability to obscure some information from being displayed in the results of an internet search of an individual's name. The court does not require the information to be taken down from the internet. The court does not prohibit the search engine from linking to the information as the result of a different query"[36] – it is worth adding, that doing so would contend with other fundamental rights, such as the right to information.

---

[34] CJEU, Google Spain v. AEPD, 2014. Available at: <http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065/> [Accessed 25 September 2020].

[35] HOFFMAN, David, BRUENING, Paula, and CARTER, Sophia. "The right to obscurity: How we can implement the Google Spain decision." NCJL & Tech. 17 (2015), p. 437.

[36] HOFFMAN, David, 2014. Europe's New Right to Be Forgotten: Not New and Not Forgetting - Policy@Intel. [online] Policy@Intel. Available at: <https://blogs.intel.com/policy/2014/07/16/europes-new-right-forgotten-new-forgetting/#gs.fis0to> [Accessed 25 September 2020].

It shall come as no surprise that there is bound to be some overlap between the right to privacy and data protection, with the latter contributing to the fulfillment of the former and vice-versa. This relationship between the two rights and their self-standing capacities will be promptly dissected in chapter V, where we will focus on LFRTs in the EU legal context.

Until that moment, this brief theoretical exposition of the ethics behind privacy and data protection, will be quintessential to fully grasp the stance of EU on facial recognition technologies. This stance will be explored later in chapter IV.

Before moving on to the EU sphere however, it is relevant to observe what jurisdictions across the Atlantic are saying regarding facial recognition technologies.

III – USE OF FACIAL RECOGNITION TECHNOLOGY OUTSIDE OF THE EU

Previously we briefly made reference to the usage of LFRTs in China, where in Hong Kong protesters are tearing down facial recognition towers to avoid being identified as dissidents by the Chinese government[37]. In the mainland, LFRTs are used for racial profiling of Muslim minorities, potentially leading to what some call "a new era of automated racism" [38].

In this chapter we will be looking westward, specifically towards Brazil and the United States of America, which display some judicial cases that are worth bringing up, as they showcase potential practical applications of the technology, but also ubiquitous issues that may arise from them.

1 – Facial Recognition technologies in Brazil

The Southern American country where a new data protection law, akin to the GDPR has entered into force in August 2020, has recently witnessed a decision from the *Tribunal de Justiça de São Paulo*[39] regarding LFRTs. The court decided on an injunction that ordered *ViaQuatro*, the entity which is responsible for that Metro Station, to cease using facial recognition technology in the city's subway. The technology detected the gender and approximate age of the citizens as well as their facial expression response towards advertisements – happy, unsatisfied, surprised or neutral. In this sense this varies from the standard LFRTs and would

[37] HAINS, Tim, 2019. Protesters in Hong Kong Tear Down Facial Recognition Towers as Violence Escalates. [online] Realclearpolitics.com. Available at: <https://www.realclearpolitics.com/video/2019/08/25/protesters_in_hong_kong_tear_down_facial_recognition_towers_as_violence_escalates.html> [Accessed 25 September 2020].

[38] MOZUR, Paul, 2019. One Month, 500,000 Face Scans: How China Is Using A.I. To Profile A Minority. [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> [Accessed 7 September 2020].

[39] Tribunal de Justiça do Estado de São Paulo, Processo Nº: 1090663-42.2018.8.26.0100, 2018. Available at: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/sp_10906634220188260100_14092018.pdf?fbclid=IwAR2kS-QU8Fm5bNOpbijV6TncqsL6E1ru1XvKQtomBdFc7Zqo_nsNpyFtjh8> [Accessed 25 September 2020].

seem at first glance less intrusive as it does not check facial images against a watchlist, nor does it capture or process personal data according to *ViaQuatro*.[40]

Notwithstanding, the court considered that the technology was violating the right to information, in the sense that it was not clear what was the exact purpose of the capture of the images or the way in which data was being processed, which, the court argued, should have been extensively explained to the subway users.

It went on to add that there were no guarantees on the digital safety standards of the data, both during its processing and storage, which could lead, among others to discriminatory behaviours, by profiling a consumer based on their race or gender and attributing benefits to one group in detriment of another.

In conclusion, the technology was deemed a tool to forcedly research public opinion, as the systems were installed in the doors of the trains – "interactive digital doors" – not allowing people to opt-in on whether to be analysed by the system – even if they were properly informed.

Two years past this decision, São Paulo saw a return of facial recognition technology, this time on a public level. On the 28th of January 2020, a Biometric Identification Laboratory was inaugurated in the city, which would allow state authorities to identify citizens in criminal investigations. The software was not a LFRT as it functioned asynchronously, comparing older photos or CCTV recordings to a database held by the State security agency, the *Secretaria de Segurança Pública*.[41]

Nonetheless, one month later in February 2020, the police were given ampler powers by the City Council, allowing them to test a dynamic live-facial recognition

[40] DEMARTINI, Felipe, 2018. Justiça Ordena Fim De Coleta De Dados Faciais Na Linha Amarela Do Metrô De SP. [online] Canaltech. Available at: <https://canaltech.com.br/seguranca/justica-ordena-fim-de-coleta-de-dados-faciais-na-linha-amarela-do-metro-de-sp-122744/> [Accessed 25 September 2020].

[41] BOSELLI, André, 2020. Polícia Paulista Usará Reconhecimento Facial Em Investigações. [online] Consultor Jurídico. Available at: <https://www.conjur.com.br/2020-jan-29/policia-paulista-usara-reconhecimento-facial-investigacoes> [Accessed 25 September 2020].

software during the São Paulo's Carnival event[42]. The watchlist was composed of 32 million faces included in the law enforcement's database and aimed at identifying fugitives and/or missing persons. Reports indicate that the first weekend of the Carnival saw 413 people being arrested, amongst which 127 were criminals identified by facial recognition technology[43].

According to the Governor of São Paulo, João Doria, the facial recognition was done not only via static cameras placed in strategic locations but was likewise carried out by fifty drones overflying the main areas of the *Sambódromo*. He further stated that "drones will be the great agents which will propel electronic surveillance"[44].

While unmanned aerial vehicles (UAV) capacitated with live facial recognition software can be extremely useful towards policing efforts, it is worth inquiring how the distance and angle at which drones capture facial images will impact the accuracy of the technology. Some authors have attested that the small-sized facial images taken by drones cause trouble on facial detection and recognition, theorizing that 3D modelling techniques might tackle these shortcomings in the future, alerting however that such claim requires further investigation[45].

There is a safeguard to these software deficiencies though. According to a General-Delegate of the Civil Police, fundamental rights and freedoms are protected, as the face matches are monitored by police officers who validate or invalidate the software's decision. Therefore, facial recognition does not have a last say on a

[42] CRUZ, Elaine Patricia, 2020. Polícia Usa Sistema De Reconhecimento Facial No Carnaval De São Paulo. [online] Agência Brasil. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-02/policia-usa-sistema-de-reconhecimento-facial-no-carnaval-de-sao-paulo> [Accessed 25 September 2020].
[43] Folha de S. Paulo. 2020. Polícia Prende 413 Pessoas No 1º Fim De Semana Oficial Do Carnaval De Rua Em SP. [online] Available at: <https://www1.folha.uol.com.br/cotidiano/2020/02/policia-prende-413-pessoas-no-1o-fim-de-semana-oficial-do-carnaval-de-rua-em-sp.shtml> [Accessed 25 September 2020].
[44] OKUMURA, Renata, 2020. Carnaval De SP Terá Drones, Reconhecimento Facial E 15 Mil Policiais Por Dia. [online] Estadão. Available at: <https://sao-paulo.estadao.com.br/noticias/geral,carnaval-de-sp-tera-drones-reconhecimento-facial-e-15-mil-policiais-por-dia,70003197829> [Accessed 25 September 2020].
[45] HSU, Hwai-Jung and CHEN, Kuan-Ta, 2015. Face Recognition on Drones. [pdf] Institute of Information Science, Academia Sinica. Available at: <https://www.researchgate.net/publication/300655333_Face_Recognition_on_Drones> [Accessed 25 September 2020], p. 43 and 44.

criminal investigation but rather is used as any other means of proof[46]. This is especially relevant since these technologies are prone to biases and misidentifications, therefore the existence of human oversight is crucial, however it is not without its own shortcomings.

Adding to this point, let us observe a famous judicial case from the U.S. that shines a brighter light on the question of the defects of human intervention in facial recognition.

2 – Facial Recognition technologies in the United States of America

In September 2014, in the U.S.A, a citizen named Steve Talley was reportedly beaten up and arrested due to his alleged connection to two bank robberies, one in May and another in September of that year[47]. A video surveillance of those robberies had been made available to the public, which led to him being identified by three acquaintances as a potential culprit.

Having proven that he was working as a financial adviser when the first robbery was taking place the charges were dropped and he was released in November 2014.

In December 2015 he was arrested once more, this time based on the robbery that took place in September. An FBI facial recognition software had been used, and an FBI expert on facial recognition had been assigned to compare the pictures of the surveillance video with several pictures of Talley. He concluded that in both instances he was looking at the same person. This was disproved once more, and Talley was released and launched a lawsuit against the FBI asking for 10 million dollars in reparations.

[46] BOSELLI, André, 2020. Polícia Paulista Usará Reconhecimento Facial Em Investigações. [online] Consultor Jurídico. Available at: <https://www.conjur.com.br/2020-jan-29/policia-paulista-usara-reconhecimento-facial-investigacoes> [Accessed 25 September 2020].

[47] KOFMAN, Ava, 2016. How A Facial Recognition Mismatch Can Ruin Your Life. [online] The Intercept. Available at: <https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/> [Accessed 25 September 2020].

Building on this case, we can draw some illations:

Firstly, it displays that even experts at facial identification can fail to correctly match a photography or a still from a surveillance camera to a person. As George Reis, a forensic video analyst, explains, this is especially dangerous, because "[i]n this field there are a lot of people who practice with absolutely no background or experience or training and have no idea what the necessary conditions for individualization are"[48]. Moreover, as the technology evolves and its error rate diminishes, there is a risk of a growingly lax attitude towards automated decisions, with human agents possibly being more reluctant to question the algorithms' results. This is called by some authors as the "automation bias":

"[t]he phenomenon of 'automation bias' suggests that automated tools influence human decisions in significant, and often detrimental, ways. Two types of errors are particularly common: omission errors, in which people do not recognize when automated systems error, and commission errors, in which people follow automated systems without considering contradictory information. Heavy reliance on automated systems can alter people's relationship to a task by creating a 'moral buffer' between their decisions and the impacts of those decisions". Thus, although "[a]utomated decision support tools are designed to improve decision effectiveness and reduce human error, [. . .] they can cause operators to relinquish a sense of responsibility and subsequently accountability because of a perception that the automation is in charge." [49]

With this in mind, we should nonetheless underscore that human agency is of the utmost importance, as, in theory, it withdraws the power of the decision from the machine lending the last word to a human. Even though in practice these humans

[48] KOFMAN, Ava, 2016. *How A Facial Recognition Mismatch Can Ruin Your Life*. [online] The Intercept. Available at: <https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/> [Accessed 25 September 2020].

[49] GREEN, Ben; CHEN, Yiling. Disparate interactions: An algorithm-in-the-loop analysis of fairness in risk assessments. In: Proceedings of the Conference on Fairness, Accountability, and Transparency. 2019, p. 2.

can suffer from the aforementioned "moral buffer", having a human overseeing the technology does foster an endeavour of trust.

This is not to say that the situation that we described should be ignored – on the contrary, such 'mind traps' should be addressed, and human agents should be properly trained, to equip them with the awareness of these possible shortcomings and a critic mind in relation to algorithmic decision-making.

Furthermore, judicial actors should also receive adequate training. It must be stressed that, just like humans, software (created by men) is bound to be imperfect. Thus, the proof resulting from a facial recognition technology match and subsequent human input, should always be followed by a due process of law, not conceding any proof the status of dogma.

Gant Fredericks, a video analyst who teaches at the Texas Forensic Science Commission, said in an interview that "[i]t is dangerous for a video examiner to tell the court that the person on video is the defendant. If it were that easy, there would be little need for trials in a surveillance society and that's a frightening thought"[50]. What Fredericks is arguing for is a shift on a binary response of "hit or miss". LFRTs are not capable of answering with one hundred percent certainty and this should not be ignored during a judicial process.

Following such arguments, some authors are clamouring for "[a] new concept of technological due process", stating that "[a]utomated systems jeopardize due process norms. Hearings are devalued by the lack of meaningful notice and by the hearing officer's tendency to presume a computer system's infallibility."[51]

[50] KOFMAN, Ava, 2016. *How A Facial Recognition Mismatch Can Ruin Your Life*. [online] The Intercept. Available at: <https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/> [Accessed 25 September 2020].
[51] CITRON, Danielle Keats, 2007. "Technological due process." Wash. UL Rev. 85, p. 1249.

In a country where in 2016 half of its population was in a law enforcement facial recognition database[52], the technology seems to be commonplace in police investigations, and more controversial usages of LFRTs by the police are being projected[53]. Despite this, in 2019 the largest manufacturer of body cameras in the U.S., Axon, announced that they would not add the technology to their cameras, following the position defended by the company's ethic board[54], which, among other recommendations, warned that the technology might lead to an encroachment of government powers on public life.

In a similar fashion, in the same year, the U.S. saw some bans on facial recognition systems, first in San Francisco and later in other American cities[55]. The basis was the technology's intrusive nature and unreliability, as well as the fact that it was considered an unnecessary infringement on privacy and liberties.

The "unreliability" argument stems from the technical biases of the technology, resulting in false-positive results[56] regarding demographics such as women, dark complexed individuals, or the elderly, who "may be subjected to disproportionate scrutiny, thereby creating a new type of 'digital divide'"[57].

Matt Cagle, a Technology and Civil Liberties attorney from the American Civil Liberties Union, applauded the decision, stating that "[w]ith this vote, San Francisco has declared that face surveillance technology is incompatible with a

[52] VALENTINO-DEVRIES, Jennifer, 2020. How the Police Use Facial Recognition, And Where It Falls Short. [online] Nytimes.com. Available at: <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html> [Accessed 25 September 2020].
[53] GERSHGORN, Dave, 2020. Exclusive: Live Facial Recognition Is Coming to U.S. Police Body Cameras. [online] Medium. Available at: <https://onezero.medium.com/exclusive-live-facial-recognition-is-coming-to-u-s-police-body-cameras-bc9036918ae0> [Accessed 25 September 2020].
[54] SCHUPPE, Jon, 2019. Should Police Body Cameras Have Facial Recognition Tech? Axon, The Largest U.S. Maker of Devices, Says No. [online] NBC News. Available at: <https://www.nbcnews.com/news/us-news/should-police-body-cameras-have-facial-recognition-tech-axon-largest-n1023271> [Accessed 25 September 2020].
[55] COWAN, Jill, 2019. San Francisco Banned Facial Recognition. Will California Follow? [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/07/01/us/facial-recognition-san-francisco.html> [Accessed 25 September 2020].
[56] There can also be false-negative results, when someone is erroneously not identified as matching an existing database.
[57] INTRONA, Lucas, and WOOD, David. "Picturing algorithmic surveillance: The politics of facial recognition systems." Surveillance & Society 2.2/3 (2004), p. 192.

healthy democracy and that residents deserve a voice in decisions about high-tech surveillance"[58].

Along the same lines, the tech giant IBM released a public statement in 2020, claiming to halt its development and offer of facial recognition software to law enforcement for purposes of "mass surveillance or racial profiling". In a letter to the American Congress, IBM chief executive wrote that the technology needs testing "for bias" and that "IBM firmly opposes and will not condone the uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms".[59]

The Brazilian and the American current technological paradigm shine a light on various issues we will further explore in this dissertation, namely the biases and error rates displayed by LFRTs and the importance of human oversight to mitigate these defects.

In the European Union, some Member States are likewise pushing for these technologies to better achieve security purposes – ignoring how accurate their software may be.

To illustrate this point, according to a leaked document[60] in late 2019, an EU Council report detailed measures proposed by Austria on a shared network of facial recognition databases for law enforcement authorities in the EU.

[58] LEE, Dave, 2019. San Francisco Is First US City to Ban Facial Recognition. [online] BBC News. Available at: <https://www.bbc.com/news/technology-48276660> [Accessed 25 September 2020].
[59] [Unknown author] BBC News. 2020. IBM Abandons 'Biased' Facial Recognition Tech. [online] Available at: <https://www.bbc.com/news/technology-52978191> [Accessed 25 September 2020].
[60] STOLTON, Samuel, 2020. EU Police Plan Massive Facial Recognition Database. [online] www.euractiv.com. Available at: <https://www.euractiv.com/section/digital/news/eu-police-plan-massive-facial-recognition-database/> [Accessed 25 September 2020.]

The document explored the possibility of including facial image data on the Prüm Treaty – which currently allows cross-border exchange and comparison of forensic DNA, fingerprint and vehicle registration amongst Member-States police.

This exchange of new forensic data modalities where facial recognition is included is not a novelty and has been discussed by academics exploring a new Prüm regime[61]. Nonetheless, it has fuelled some concerns of civil rights actors in the EU.

Edin Omanovic, advocacy director for Privacy International, has expressed his concerns regarding this expansion of the Prüm Treaty, "especially as some EU countries veer towards more authoritarian governments", which leads Omanovic to fear that this European LFRTs database can be used for "politically motivated surveillance", rather than standard law enforcement[62].

This directs us to the fact that this is a highly politized technology, raising concerns that it might be misused to push for surveillance states. Thus, it is highly relevant to delve into the world of policymaking that has been developing in Brussels since the GDPR came into effect, namely investigating the European Commission's stance to foster trust in EU citizens regarding artificial intelligence in general and facial recognition technologies in particular.

[61] TOOM, Viktor, 2018. Cross-Border Exchange and Comparison of Forensic DNA Data in The Context of The Prüm Decision. [pdf] European Parliament's Committee on Civil Liberties, Justice and Home Affairs. Available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf ,> [Accessed 25 September 2020], p. 40, 44 and 45.

[62] CAMPBELL, Zach and JONES, Chris, 2020. Leaked Reports Show EU Police Are Planning A Pan-European Network of Facial Recognition Databases. [online] The Intercept. Available at: <https://theintercept.com/2020/02/21/eu-facial-recognition-database/> [Accessed 25 September 2020].

IV – THE PATH TOWARDS TRUSTWORTHY ARTIFICIAL INTELLIGENCE IN THE EU – A POLITICAL CONTEXT ANALYSIS

While the EU is considerably behind China or the USA in terms of AI innovation and development, it has made its priority to strengthen the aspect of trustworthy AI by following "ethical guidelines and transparent criteria"[63] hoping that this could be the "silver bullet"[64] that could differentiate the EU. This philosophy and strategy effectively set the tone for the legislative approach that will most likely impact facial recognition technologies.

While this dissertation does not aim to fulfill a prospective nature in terms of a potential future legislation, analyzing the European Commission's stance in regard to LFRTs will reward us with hints on what the future of the technology might be – or even grasp whether the technology has a place in Europe's future.

Towards this end, we will be analyzing some of the most relevant documents released from 2018 to 2020 by the European Commission, as well as commentaries from some key political actors in the "*Euro bubble"*.

Starting in 2018, we will begin with the first High-Level Expert Group on Artificial Intelligence (AI HLEG), created with the goal of "maximising the benefits and minimising the risks of AI"[65].

This group of 52 experts from various fields was responsible for an initial draft named "Ethics Guidelines for Trustworthy AI" which was released on the 18th of December 2018 and was made available for open consultation and feedback. On the 8th of April 2019 the non-binding document was disclosed to the public, after feedback from over five hundred contributors.

[63] DELCKER, Janosch, 2019. Europe's Silver Bullet in Global AI Battle: Ethics. [online] POLITICO. Available at: <https://www.politico.eu/article/europe-silver-bullet-global-ai-battle-ethics/> [Accessed 25 September 2020].
[64] Ibid.
[65] ALA-PIETILÄ, Pekka, 2019. Towards Trustworthy AI - Ethics & Competitiveness Go Hand-In-Hand. [online] Available at: <https://ec.europa.eu/digital-single-market/en/blogposts/towards-trustworthy-ai-ethics-competitiveness-go-hand-hand> [Accessed 25 September 2020].

An analysis of the end-product will be most valuable, as it laid down the foundations that have since been transposed to more recent documents on this subject.

After scrutinizing the guidelines from the Expert Group, we shall observe the political guidelines of the current President of the European Commission, as well as the 2020 European Strategy for Data and the 2020 white paper on Artificial Intelligence.

1 – Ethics Guidelines for Trustworthy AI[66] – An analysis of the framework written by the High-Level Expert Group on Artificial Intelligence

The analysis of these guidelines will serve the purpose of providing us with a first interaction with the notion of "trustworthy AI" – and consequentially, trustworthy LFRTs. This document sets the scene for the white paper on Artificial Intelligence, released in February of 2020, which we will explore shortly after.

For this reason, the analysis will be brief, but sufficiently thorough, so that the reader will be able to not only grasp how AI will most likely fit in the regulatory framework of the EU, but also fathom the context that surrounds the contents within the white paper.

We should start by underscoring that to achieve trustworthy LFRTs, one must not ignore the underlying ethical issues. Ethics guidelines becomes even more relevant, if we consider that this technological field is highly volatile, with technological advances being swifter than legislative ones, thus leading to potential legislative voids.

[66] Artificial Intelligence High-Level Expert Group, Ethics Guidelines for Trustworthy AI, 2019 [online] PDF available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation> [Accessed 25 September 2020].

Let us then delve into a brief exposition of this document, which begins by asserting that trustworthy AI needs to have three harmonious components[67]:

1) be **lawful**, "complying with all applicable laws and regulations";
2) be **ethical** "ensuring adherence to ethical principles and values", drawing from fundamental rights enshrined in the EU (e.g. respect for human autonomy; prevention of harm; fairness);
3) be **robust** "both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm."

Secondly, it claims that AI should be implemented only if it meets seven key requirements. These will vary in levels of importance, regarding the sector or industry we are analyzing, but should be equally important to consider throughout the life cycle of the AI system concerned.

The requirements are as follows: 1) human agency and oversight; 2) technical robustness and safety; 3) privacy and data governance; 4) transparency; 5) diversity; 6) non-discrimination and fairness, societal and environmental wellbeing; and 7) accountability.

In its work, the AI HLEG concludes that some legislative pieces will need to be "revised, adapted and introduced, both as a safeguard and as an enabler"[68]. Specifically, regarding the topic of this dissertation, it is worth noting that the Expert Group's individualize LFRTs as a "critical concern raised by AI", mentioning that even in circumstances where legal basis might seem to be covered, there may exist some possible ethical grey areas. The experts call for a proportionate usage of biometric technologies, as to uphold the autonomy of citizens of the EU, as well as a clear definition of "when and how can AI be used for automated identification of individuals and differentiating between the

[67] Artificial Intelligence High-Level Expert Group, Ethics Guidelines for Trustworthy AI, 2019 [online] PDF available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation> [Accessed 25 September 2020], p. 2.
[68] Ibid., p. 22.

identification of an individual *versus* the tracing and tracking of an individual, and between targeted surveillance and mass surveillance"[69], which the authors defend is crucial if we are to achieve trustworthy facial recognition in the EU.

This brief exposition allows us to understand why the High-Level Expert Group has called this a "human-centric" approach, rather than a purely economic one, as it promotes human welfare and freedom, while being sufficiently dynamic as to adapt to the volatility of AI.

In essence, the framework claims for AI seen through a lens of respect for fundamental rights, democracy and the rule of law, as enshrined in the Treaties and the Charter, as well as in international human rights law.

This approach is, evidently, not without critics – Daniel Castro, vice-president of the Information Technology and Innovation Foundation (ITIF), a think-tank with members from Google, Apple, Amazon or Microsoft, has said that this is a "softball" and "naïve approach" that will only lead to an increasingly bigger gap between the EU and the US or China.[70]

Following his philosophy, consumers are only concerned with effectiveness, and if the EU follows the ethics-first path it will fall behind its competitors.

As thought-provoking as the commentary of Castro might be, it fails to grasp the EU strategy. As stated by a member of the AI HLEG, Pekka Ala-Pietilä, there are three broad areas where AI plays a role: business to consumer (B2C), business to business (B2B) and public to citizens. He agrees that the first is dominated by the

[69] Artificial Intelligence High-Level Expert Group, Ethics Guidelines for Trustworthy AI, 2019 [online] PDF available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation> [Accessed 25 September 2020], p. 33 and 34.

[70] DELCKER, Jasnosch, 2019. Europe'S Silver Bullet in Global AI Battle: Ethics. [online] POLITICO. Available at: <https://www.politico.eu/article/europe-silver-bullet-global-ai-battle-ethics/> [Accessed 25 September 2020].

US and China; however, the ethical path might be the edge the EU needs to succeed on the two remaining areas[71].

The hint that the EU will prioritize trust over efficiency is good news for civil liberties advocates, and especially, for European citizens.

Throughout the framework, it is repeatedly underscored that Europe should be the home and leader of "ethical technology", but whether that will end up being the case is a different subject.

The disclaimer should be made that the topic of AI-oriented legislation is not a novelty, however, recently it has begun to permeate the legislative mainstream of Brussels. This Expert-Group is but a hint of that movement, one that has gained even more visibility after the current President of the European Commission, Ursula von der Leyen, set out her team's political guidelines for 2019-2024[72].

2 – **European Commission stance on AI enabled technologies**

"I want Europe to strive for more by grasping the opportunities from the digital age within safe and ethical boundaries" – it was with this assertion that the current President of the European Commission began her chapter dedicated towards "A Europe fit for the digital age", the agenda that was delivered in December 2019 and set the tone for the mandate of the new President of the EC.

In this initial approach to the topic, the President underscored the need to establish new standards for new technologies, while upholding the importance that data and AI have in improving our lives. To benefit from these technologies, a "European

[71] ALA-PIETILÄ, Pekka, 2019. Towards Trustworthy AI - Ethics & Competitiveness Go Hand-In-Hand. [online] Available at: <https://ec.europa.eu/digital-single-market/en/blogposts/towards-trustworthy-ai-ethics-competitiveness-go-hand-hand> [Accessed 25 September 2020].

[72] VON DER LEYEN, Ursula, 2019. A Union That Strives for More - My Agenda for Europe. [pdf] Brussels. Available at: <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf> [Accessed 25 September 2020].

way" has to be found, "balancing the flow and wide use of data while preserving high privacy, security, safety and ethical standards" [73].

Lastly, she concluded by asserting that new legislation regarding a coordinated European approach on the human and ethical implications of AI would be put forward in her first one hundred days in office. Since the 1st of December 2019, over one hundred days have passed, which calls for an analysis of what has been done in this domain.

On the 19th of February 2020, a press release titled "Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence"[74] was unveiled. Therein, the Commission announced the release of a white paper[75] regarding policy options to achieve "trustworthy technology", as well as a data strategy[76] that focuses on a human-centric development of AI.

This denotes that, as we have already claimed before, the work of the expert group was used as the foundations for the President's digital policy agenda regarding AI and, consequentially, the documents that the EC has since released.

The following subchapters will scrutinize the content of the mentioned Communication: firstly, regarding the European data strategy and, secondly, the white paper, in so far as it is relevant towards this dissertation's topic.

---

[73] VON DER LEYEN, Ursula, 2019. A Union That Strives for More - My Agenda for Europe. [pdf] Brussels. Available at: <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf> [Accessed 25 September 2020], p. 13.

[74] 2020. Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence. European Commission [online] Available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273> [Accessed 25 September 2020].

[75] 2020. WHITE PAPER on Artificial Intelligence - A European Approach to Excellence and Trust [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [Accessed 25 September 2020].

[76] 2020. A European Strategy for Data. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> [Accessed 25 September 2020].

2.1 – The 2020 European Strategy for Data

As we have previously pointed out, the issue at hand with facial recognition technologies in Europe is the existence of very strict rules regarding personal data, which are essential for machine learning. If these data do not exist, AI will be harder to train in the EU, leaving LFRTs created in the old continent with potential biases that can lead to discriminatory results.

This leads some European tech firms to assert that such "data desert"[77] is putting them at a disadvantage on a global scale[78]. This much has also been said by one of the experts at AI HLEG, Loubna Bouarfa, who in 2019 argued that the full potential of AI technology is hard to explore against such data barriers.[79]

As a consequence, there was a push for a new data strategy that could put Europe in the race against China and the US with lobbies clamoring for more relaxed data protection laws.

Amidst that context, the Commission felt it was time for a recap on its strategy regarding data, two years after the GDPR came into effect. This brings us to the 2020 European strategy for data, which outlines a strategy to enable the data economy for the five years to come.

The analysis we will conduct shall serve a substantial purpose in understanding how LFRTs are to be regulated. Therefore, the caveat should be made that the analysis of this Communication will not be extensively done, but only in so far as it is relevant towards the topic at hand.

Consistent with the philosophy that has been showcased in the last subchapters, it begins by underscoring the necessity of enshrining the trust of EU Citizens in data-driven innovations, which should be achieved through compliance with data

[77] DELCKER, Janosch, 2019. Europe'S Silver Bullet in Global AI Battle: Ethics. [online] POLITICO. Available at: <https://www.politico.eu/article/europe-silver-bullet-global-ai-battle-ethics/> [Accessed 25 September 2020].
[78] Ibid.
[79] Ibid.

protection rules, as well as seeing the interests of citizens through a lens of EU values and fundamental rights.

It is highlighted that data volumes are expected to rise from 33 zettabytes in 2018 to 175 zettabytes in 2025, which leads the authors to call data "the lifeblood of economic development"[80]. Likewise, the aforementioned necessity of more data availability is stressed.

It goes on to recognize that competitors like China and the US are quickly innovating and that the EU has the potential to be successful in the "data-agile economy"; however, in order to do so it must find the "European way", which will necessarily encompass a balance between the usage of data, while "preserving high privacy, security, safety and ethical standards"[81].

The vision that is laid out is human-centric and includes plans on the creation of a "single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data (…), are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data"[82], a space ruled by EU law, where attractive policies can provide some magnetism towards tech companies.

This digital ecosystem has the potential to bolster EU technological sovereignty, shaping the digital space in compliance with EU values. Such goal, if effectively reached, would create an area in which "data deserts" are no longer a concern, allowing LFRTs to grow through machine learning, and exist in a properly regulated and controlled environment.

This is of course an idyllic approach to the issue. To put into practical terms these hopes and dreams of the current Commission, some problems will have to be

[80] 2020. A European Strategy for Data. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> [Accessed 25 September 2020], p. 2.
[81] Ibid., p. 3.
[82] Ibid., p. 4 and 5.

tackled during the process. One of these issues is the infrastructural dependency of the EU, which relies on US and China's servers to store data – this is especially relevant for our topic, as LFRTs' databases require adequate and secure cloud storage.

This issue has not been overlooked in the Communication regarding the Strategy for Data of the EU. In it, the Commission showed no naivety, assuming its shortcomings and laying down a plan to counter that dependency:

"The digital transformation of the EU economy depends on the availability and uptake of secure, energy-efficient, affordable and high-quality data processing capacities, such as those offered by cloud infrastructures and services, both in data centres and at the edge. In this perspective, the EU needs to reduce its technological dependencies in these strategic infrastructures, at the centre of the data economy".[83]

To counter these dependencies, the Commission will invest €4-6 billion in a "High Impact Project on European data spaces and federated cloud infrastructures", in order to address the deficiencies existent in the data-sharing and AI ecosystems, which "will address the specific needs of industries in the EU, including hybrid cloud deployment models that allow data processing at the edge with no latency (cloud-to-edge)"[84].

This strategy effectively aims to solve one of the biggest deficiencies regarding the integrity and confidentiality of personal data in the EU.

Consequentially, it seeks to bolster the attractiveness of EU in the data-agile economy, which shall be achieved by pursuing a "European way" of addressing data. The creation of independent European cloud infrastructures, as well as Common European data spaces, harmoniously regulated across the board, sets a

[83] 2020. A European Strategy for Data. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> [Accessed 25 September 2020], p. 9.
[84] Ibid., p. 16.

backdrop where the development of facial recognition systems can potentially thrive in a controlled and trustworthy environment.

2.2 – The White Paper on AI – "A European approach to excellence and trust"

The white paper, released jointly with the Communication, seeks to sediment the stance of the new Commission regarding AI, revisiting the document produced in 2018 by the AI HLEG as well as a Communication of April of the same year[85].

AI and data economy go hand in hand; therefore, it is no surprise that the data strategy covered previously overlaps in a lot of areas with this white paper. Notwithstanding, it does add some nuances that contribute towards this holistic view, laying out policy options that will enable the EU to promote AI while addressing the risks of such technology.

With that being said, the document in question begins by asserting "trustworthiness" as a prerequisite for the uptake of AI, with talks of the construction of a "trust ecosystem" – this in itself is coherent with the previous analysed works, making it clear that the EU strategy, is, as was speculated initially, marketing ethics as a "silver bullet"[86] against competitors.

The Paper holds lack of trust as one of the main accountable factors to the lack of innovation in AI in the EU, contending that citizens who worry that AI can have unintended effects or be used maliciously will be hesitant to approve of said technologies.

Nonetheless, it affirms the importance that AI enabled technologies can have in defending the public interest, ensuring the security of citizens against threats such as that of terrorism. However, it does not fall short on voicing an explicit concern

[85] 2018. COM (2018) 237 final. Artificial Intelligence For Europe. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF> [Accessed 25 September 2020].

[86] DELCKER, Janosch, 2019. Europe's Silver Bullet In Global AI Battle: Ethics. [online] POLITICO. Available at: <https://www.politico.eu/article/europe-silver-bullet-global-ai-battle-ethics/> [Accessed 25 September 2020].

regarding data protection and privacy rights, when it comes to the use of AI in law enforcement, since this is an area in which citizens' rights are at a greater risk of jeopardy.

More specifically, the white paper goes on to mention the risk of AI being used for mass surveillance in breach of EU data protection and other rules, be it by state authorities or employers observing the behaviour of employees. Furthermore, it underscores that face recognition systems have the added issue of displaying gender and racial biases (low error rate for light-skinned men contrasted to a higher rate of error regarding darker-skinned women). In doing so, it concedes that AI can lead to material as well as immaterial harms, such as loss of privacy, freedom of expression, human dignity or result in discrimination.

The Commission argues that the current "legislative framework could be improved"[87] so that the risks posed by AI are mitigated through an adequate regulatory mantle that safeguards fundamental rights. In its conclusion, the EC adds that "in addition to the possible adjustments to existing legislation – a new legislation specifically on AI may be needed in order to make the EU legal framework fit for the current and anticipated technological and commercial developments."[88] This means that as well as a new legislation on AI, already existent one such as the GDPR will most likely be seeing some tweaks, to better accommodate facial recognition technologies.

Regarding the future regulatory framework for AI, the Commission states that it should follow a "risk-based approach" to ensure a proportionate interventionism. This requires an analysis of what a "high-risk" AI application is. While the paper presents cumulative criteria to assess the risk of AI applications, it underscores the importance of considering some AI applications as intrinsically high-risk. The

[87] 2020. WHITE PAPER on Artificial Intelligence - A European Approach to Excellence and Trust. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [Accessed 25 September 2020], p. 14.
[88] Ibid., p. 16.

example given is that of remote biometric identification used to determine the identities of multiple persons in a public space – the same is to say that **the Commission considers LFRTs as a high risk AI application** that will be regulated by this specific AI legislation.

This future regulatory framework will impose some legal requirements that will apply at "all times" to high-risk AI. Among these potential requirements, which draw from the initial seven requirements earlier presented by the AI HLEG, the white paper lists the following[89]:

- Training data;

- Data and record-keeping;

- Information to be provided;

- Robustness and accuracy;

- Human oversight;

- Specific requirements for certain particular AI applications, such as LFRTs.

It is worth mentioning that these legal requisites are but a draft provided by the EC, as to kickstart the legislation on AI that was promised on von der Leyen's political agenda.

So far, contrary to the one hundred days goal that the Commission was set to achieve, there has been no specific EU legislation that rules over AI in general and LFRTs in particular. However, considering the complexity of the matters at hand, the approach of the EC seems to be the most prudent – rather than rushing towards

[89] 2020. WHITE PAPER on Artificial Intelligence - A European Approach to Excellence and Trust. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [Accessed 25 September 2020], p. 18.

half or extreme measures (the Commission initially considered a ban of up to five years in remote facial recognition).[90]

The horizon seems to hold changes to legislations, changes that will hopefully address many of the issues discussed and to be discussed throughout this dissertation. Notwithstanding, it becomes clear that the *sui generis* nature of LFRTs demand an answer that goes beyond updating existing legislations, an answer that hopefully will be brought under the wing of the new regulatory framework for AI.

[90] BBC News. 2020. Facial Recognition: EU Considers Ban of up to Five Years. [online] Available at: <https://www.bbc.com/news/technology-51148501> [Accessed 25 September 2020].

V – LIVE FACIAL RECOGNITION TECHNOLOGIES IN THE EU LEGAL CONTEXT

The following chapter aims to observe and critic the current legal framework in the EU, as well as some decisions from its Member States' Courts and Data Protection Authorities (DPA), in so far as they are relevant for the topic at hand. It will begin with a more general view of the fundamental rights that come into play when considering LFRTs; after this initial approach, we will delve into data protection laws such as the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Directive). Our purpose is to ascertain whether these legislative pieces are fit to accommodate LFRTs as they stand and identifying potential loopholes.

1 – Impact of Live Facial Recognition Technology on Fundamental Rights

While facial recognition can be highly beneficial towards crime prevention or finding missing persons, as we have previously witnessed, this is not without its own shortcomings and flaws. Many watchdogs are therefore concerned about this other side of the coin, namely the enjoyment of fundamental rights and freedoms that such technologies can curtail. Some of these rights have already been tacitly or expressly mentioned in previous chapters, nonetheless, it is worthwhile to inquire further and expressly on what rights are at risk, as well as which rights can serve as legal justification for or against LFRTs.

1.1 – Human dignity

Let us begin by addressing the foundational right to human dignity, asserted in article 1 of the Charter of the Fundamental Rights of the European Union. This principle expresses "that each human being possesses an intrinsic worth that should be respected, that some forms of conduct are inconsistent with respect for

this intrinsic worth, and that the state exists for the individual not vice versa"[91]. This intrinsic worth may be at risk of jeopardy if we think about the potential subjugation of human beings to the will of algorithms.

1.2 – Right to security

Article 6 of the Charter lays down the right not only to liberty, but also to security – physical security of the population being a value that the CJEU considers as an objective of general interest[92], with the Court calling upon that article when pondering over such value[93].

With this fundamental right as the backdrop, crime prevention becomes a catalyst to fulfil this right, therefore assuming itself as an objective of general interest[94]. LFRTs can be an essential tool in preventing crime, finding missing children or elderly, thus, have the potential to be a technology oriented towards the security of individuals.

1.3 – Freedom of expression and assembly

Freedom of expression and assembly are separately postulated on article 11 and article 12 of the Charter. While the impact of LFRTs on these rights might not be evident, a clear example can be seen when examining the case of the protesters in Hong Kong in 2019[95], who were allegedly being identified by LFRTs.

[91] MCCRUDDEN, Christopher. Human dignity and judicial interpretation of human rights. european Journal of international Law, 2008, 19.4, p. 723.
[92] For example, Case C-145/09 Tsakouridis EU:C: 2010:708, paragraphs 46 and 47.
[93] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014., paragraph 42.
[94] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014., paragraph 44.
[95] MOZUR, Paul, 2019. In Hong Kong Protests, Faces Become Weapons. [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html> [Accessed 25 September 2020].

This impossibility of anonymously protesting can and will have a chilling effect[96] – an inhibition or discouragement of the legitimate exercise of a legal right due to the fear of the legal sanction[97] – on the freedom of expression and assembly, as it can result in a voluntary withdrawal from society to escape surveillance, for fear of repercussions for being a political dissent.

The impact LFRTs can have on our possibility to freely join political protests is an effective deterrent to a democratic society and is a strong argument against the technology.

1.4 – Right to not be discriminated against

Article 21 of the Charter lays down the non-discrimination right that reads as follows:

"1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

Again, it might not be immediately entirely foreseeable how LFRTs can lead to discrimination, after all, technology is neutral (or is it?).

The most apparent situation of intended discrimination can occur on the programming of the software, e.g. programming it to only identify people belonging to an ethnic minority.

However, discrimination can result from biases that the software developed by itself. To understand how this can occur we need to look at machine learning in AI, namely to the so called "black box effect" or the issue of AI's opacity. What

[96] [Unknown author] Privacyinternational.org. n.d. Facial Recognition | Privacy International. [online] Available at: <https://privacyinternational.org/learn/facial-recognition> [Accessed 25 September 2020].
[97] Yourdictionary.com. n.d. Chilling-Effect Dictionary Definition | Chilling-Effect Defined. [online] Available at: <https://www.yourdictionary.com/chilling-effect#law> [Accessed 25 September 2020].

this means is that the algorithm is given inputs regarding data, through which it learns and produces outputs – while we have control over the input of data, the same control is not so easy to obtain regarding output results that derive from the machine-reasoning process itself.

This can lead to an algorithm producing discriminatory results that were not intended or expected by the data scientists or programmers, a common issue in LFRTs.

Moreover, it is worth mentioning that LFRTs in the EU will, in principle, require a human agent to validate the software's match – as we mentioned previously, human oversight is a potential legal requirement of trustworthy AI in the EC's white paper. This means that it is not enough that the technology identifies an individual, the last voice will have to come from human intervention. In such situations, the existence of discriminatory behaviour can be easier to perceive.

On the point of discriminatory behaviour regarding LFRTs, it is crucial to analyse the judicial case of *R (Bridges) v CCSWP and SSHD*[98].

a) The case of R (Bridges) v CCSWP and SSHD

In September of 2019, the High Court in Cardiff was the stage for the first EU judicial decision regarding the usage of LFRTs in the case of *R (Bridges) v CCSWP and SSHD*.

The issue at hand was the usage of facial recognition technology by the South Wales Police (SWP). The claimant, Mr. Edward Bridges, asserted, amongst other points, that the technology was contrary to the Equality Act 2010, as the technology had the potential of being indirectly discriminatory – as we have previously noted.

[98] HIGH COURT OF JUSTICE QUEEN'S BENCH DIVISION DIVISIONAL COURT SITTING AT CARDIFF CIVIL JUSTICE CENTRE, R (Bridges) v Chief Constable of the South Wales Police, 2019. Judiciary.uk. Available at: <https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf> [Accessed 25 September 2020].

The Court found that in April 2017 when the LFRT trial commenced, there was no suggestion that the SWP recognised or ought to recognise that the facial recognition software it had licenced might operate in a way that was indirectly discriminatory. Even if it had, the Divisional Court added that there was no firm evidence that the software produced indirect discrimination. The reasoning of the Court was that, in accordance with the expert witness's statement, the accuracy of the technology could only be judged by observing the datasets used to train it. Since the claimant had no access to the datasets, he could not make such a claim (par. 153).

Nonetheless, the same witness concluded that "bias has been found to be a feature of common [LFRT] systems" (par. 155). Responding to these claims, an officer of the SWP's Digital Services Division explained he had reviewed the use of the technology and that his results suggested no biases (par. 154).

Moreover, the Court asserted that an important failsafe was in place as "no step [was] taken against any member of the public unless an officer (the systems operator) [had] reviewed the potential match generated by the software and reached his own opinion that there [was] a match between the member of the public and the watchlist face" (par. 156).

While this in itself is generally a good way to combat erroneous results, as we have seen before and according to research, "information presumed to help people make fairer decisions can fail to do so because it filters through people's preexisting biases."[99] This means that human intervention can end up leading to a blindfolded validation of the machine's results, because the result is in line with the stereotypes the human agent possesses.

Notwithstanding, in consonance with the reasoning the Court alluded to (and some others which we chose not to delve into yet), the Claimant's petition for judicial review was dismissed on all grounds, with the Court finding that the current legal

[99] GREEN, Ben; CHEN, Yiling. Disparate interactions: An algorithm-in-the-loop analysis of fairness in risk assessments. In: Proceedings of the Conference on Fairness, Accountability, and Transparency. 2019, p. 2.

framework was adequate to accommodate an appropriate and non-arbitrary use of the facial recognition technology (par. 159).

Considering what we have been exposing during this dissertation this decision might be unexpected. However, it is worth noting that it does not reflect the final decision of the UK's jurisprudence.

The aforementioned decision was appealed by Mr. Edward Bridges and the decision of the Court of Appeal was delivered in August 2020[100]. This means that this is a post-Brexit decision, despite that, it is worth noting what the final decision from this Court was.

The claimant went on to appeal on various grounds, one of which being that the Divisional Court had erred in considering that the SWP had complied with the Public Sector Equality Duty, which requires public bodies to have due regard to the need to eliminate discrimination[101]. In his appeal, Mr. Bridges claimed that he did not seek to allege specifically that the software used by SWP was biased, rather he complained that the SWP failed to fulfil its positive obligation to obtain information on whether their software had biases or not (par. 185).

Given the circumstances, the Court concluded in favour of Mr. Bridges, considering that as LFRTs are "a novel and controversial technology, all police forces that intend to use it in the future [should] wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias" (par. 201).

[100] COURT OF APPEAL (CIVIL DIVISION), R (Bridges) v Chief Constable of the South Wales Police, 2020 Available at: <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> [Accessed 25 September 2020].

[101] GOV.UK. n.d. Review of Public Sector Equality Duty. [online] Available at: <https://www.gov.uk/government/groups/review-of-public-sector-equality-duty-steering-group> [Accessed 25 September 2020].

As a final remark that will bridge our transition to the next section of this chapter, the Court of Appeal also found that the use of LFRTs by the SWP was not compatible with the right to respect for private and family life under article 8 of the European Convention on Human Rights.

In the next section we will analyse this right in the EU legal context (postulated in the Charter of Fundamental Rights of the European Union), as well as the right to protection of personal data.

1.5 – Respect for private and family life and protection of personal data

The respect for private and family life and protection of personal data are at the forefront of the current discussion. Despite their differences, both rights have similar grounds that justify dissecting them jointly.

These fundamental rights are, at a first glance, at greater risk in relation to LFRTs, be it when an image is being used to train a software through machine learning on how to better identify facial features, when the software checks a facial image against a database or the mere existence of the said database or "watchlist" and the process through which it was formed.

With the Lisbon Treaty, the Charter of Fundamental Rights of the European Union became legally binding, at the same level as EU primary law Treaties. This formally brought the respect for private and family life and protection of personal data to the sphere of legally recognised fundamental rights of the EU.

Following this introduction, let us then observe both rights, how they relate to each other and the essential part they play in safeguarding fundamental rights.

Firstly, protection of privacy has been deemed a "classic" right, whereas data protection is a "modern" and active right[102]. While the former asserts a general

[102] CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, paragraph 71.

prohibition on interference, that can be limited if such is in line with the public interest, the latter deploys "a system of checks and balances to protect individuals whenever their personal data are processed"[103].

The right to privacy stems from the 1948 Universal Declaration of Human Rights (UDHR), where it can be read in article 12 that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

The right to privacy is first postulated in 1950 in article 8 of the European Convention on Human Rights (ECHR), stating that "[e]veryone has the right to respect for his private and family life, his home and his correspondence". In EU law, the right to privacy is enshrined as an EU fundamental right in article 7 of the Charter, asserting that "[e]veryone has the right to respect for his or her private and family life, home and communications".

On the other end of the spectrum, the right to the protection of personal data is enacted for the first time[104] in EU law under the Data Protection Directive of 1995. The right can be found on article 16 of the Treaty of the Functioning of the European Union and while deeply tied with the right to privacy, it has gained the status of independent fundamental right on article 8 of the Charter, wherein the core values of the right are laid down:

"2. Such [personal] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid

[103] BOILLAT, Philippe; KJAERUM, Morten. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, 2014, p. 19.
[104] Notwithstanding, in 1981 the Council of Europe opened for signature the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) becoming the first (and so far, the only) legally binding international instrument in its field.

down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

Data protection achieved increased public notoriety recently, when the GDPR came into effect in 2018, derogating the 1995 Directive.

It should be noted that data protection rules will be triggered if any processing of personal data is conducted. The same cannot be said about the right to private life, where to ascertain whether an intrusion has occurred with that right, the context and facts of the case need to be observed. For this reason, protection of personal data is broader than the protection conferred to private life, operating on its own, even without any breach on private life.

Recital 4 of the GDPR adds that "[t]he right to protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights". Article 1 (2) goes on to add that the GDPR protects fundamental rights and freedoms in general, and in particular the right to the protection of personal data.

The aforementioned sheds light on the fact that data protection rights' breadth goes beyond a stand-alone value, acting as an enabling right[105], forming a prerequisite to the development of the individual freedoms such as the freedom of thought, conscience and religion (article 10 of the Charter), freedom of expression and information (article 11) or freedom of assembly and of association (article 12).

Privacy rights are equally crucial on enabling these fundamental rights, with some authors going as far as considering privacy as a way to facilitate non-

[105] OOSTVEEN, Manon; IRION, Kristina. The golden age of personal data: How to regulate an enabling fundamental right? In: Personal Data in Competition, Consumer Protection and Intellectual Property Law. Springer, Berlin, Heidelberg, 2018. p. 1.

discrimination (article 21), by obscuring the information that could lead to discriminatory behaviours[106].

Moreover, in the ECtHR's case law we can read that "[t]he Court also reiterates that "private life" is a broad term, encompassing, *inter alia*, aspects of an individual's physical and social identity, including the right to personal autonomy"[107].

Article 7 of the GDPR is also crucial in enabling and safeguarding personal autonomy. In that article we can read that "[n]atural persons should have control of their own personal data". Truthfully, the importance of consent is not the only instance in which the GDPR fortifies personal autonomy. Transparency plays an equally important part, as it allows an individual to make a well-informed decision, fully knowing the consequences that his or her data's processing will entail.

It becomes evident that data protection and privacy work in a holistic effort that includes other fundamental rights, acting as pieces of a puzzle that cannot be seen separately, but rather as part of a whole.

Following this exposition, we reach the conclusion that LFRTs do not only have the capacity to affect stand-alone rights of privacy and data protection, but that forsaking these rights can lead to a rippling effect that will affect human dignity and freedom[108]. However, it should not be forgotten that these are not absolute rights, they can be limited if such is necessary to achieve an objective of general interest or to protect fundamental rights and freedoms of other citizens. Therefore, bringing them to the argumentative table against LFRTs is not a guaranteed bar on the technology. Rather, the implementation of the technology must be done in such a way that preserves the inalienable core of the fundamental rights it can pose a danger to. The same is to say that it must be subordinated to a proportionality and

[106] ROBERTS, Jessica L. Protecting Privacy to Prevent Discrimination. Wm. & Mary L. Rev., 2014, 56, p. 2173.
[107] ECtHR, Tysiac v Poland (case 5410/03), 2007, paragraph 107.

necessity test, with a legal basis to sustain its deployment, usage and legitimate aim.

In the context of the limitation of fundamental rights and freedoms to satisfy objectives of general interest, it is worth delving into two judicial cases: firstly, the case of *S. and Marper v. the United Kingdom*[109] and secondly, the case of *Digital Rights Ireland*[110].

a) The Judicial case of S. and Marper v. the United Kingdom

In 2008 the ECtHR pronounced itself regarding the judicial case of *S. and Marper v. the United Kingdom*. While not EU law *per se*, the ruling of the ECtHR sheds light on the Court's interpretation of article 8 of the ECHR. Understanding this interpretation will aid our comprehension of the second judicial case.

This ruling concerned a case where sensitive personal data (cellular samples and DNA) had been retained by law enforcement authorities after two individuals had been acquitted of their crimes. The decision held that the retention of data contended with the citizens' right to private life stated in article 8 of the ECHR.

Limitations to article 8 ECHR are allowed, as long as they are in "accordance with the law" or "prescribed by law" and are "necessary in a democratic society". In this assessment "the Court often needs to balance the applicant's interests protected by Article 8 and a third party's interest protected by other provisions of the Convention"[111]. Article 8(2) elaborates on what can be considered legitimate aims that justify the limitation of the right to private and family life: "in the interests of national security, public safety or the economic well-being of the

[109] ECtHR, S. and Marper v. the United Kingdom (30562/04 and 30566/04), 2008.
[110] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014.
[111] Guide on Article 8 Of the European Convention on Human Rights (2020) [pdf] Council of Europe/European Court of Human Rights, p.6. Available at: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> [Accessed 25 September 2020].

country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others".

In its ruling the ECtHR weighed the interests of the individuals, namely their right to privacy under article 8, *versus* the general interest of crime prevention, concluding that a "fair balance between the competing public and private interests" (par. 118) had not been achieved.

The Court criticised the blanket and indiscriminate nature of the power to retain fingerprint and DNA samples, as such could happen irrespective of the gravity of the offense or age of the offender and for an indefinite time (par. 119).

It further "observed that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests" (par. 112).

The conclusion was that new technologies need to be balanced with the benefits that can potentially be harvested from them, and their impact on fundamental rights. In that specific instance, it was found that the risk-benefit from having a database which indiscriminately stored DNA samples of individuals who had been suspected, but not convicted of a crime, was disproportionate and was not necessary in a democratic society (par. 125).

This case law provides some interesting insights regarding the ECtHR potential stance regarding LFRTs (e.g. par. 112). The Court defends that fundamental rights that can be affected by these technologies must be faced with a three-pronged proportionality test. Such test ascertains 1) whether the technology pursues a legitimate aim; 2) if it stems from law; and if it is 3) necessary in a democratic society. Regarding this last requirement, as the Court asserts, "(…) "necessary" in this context does not have the flexibility of such expressions as "useful",

"reasonable", or "desirable", but implies the existence of a "pressing social need" for the interference in question"[112].

As the European Union Agency for Fundamental Rights denotes in its focus paper on facial recognition technologies[113], the more intrusive the technology is, the stricter the proportionality test must be.

b) ***The judicial case of Digital Rights Ireland[114]***

In 2014 the Court of Justice was called upon to pronounce itself in the *Digital Rights Ireland* case, regarding the validity of the Data Retention Directive (Directive 2006/24/EC) due to its interference with article 7 and 8 of the Charter.

The Directive's subject matter concerned the combat of serious crime (such as terrorism), by retaining some publicly available data from electronic communications services or of public communications networks.

Digital Rights brought an action before a national court, in which it contested the legality of the Directive, which required, in Ireland's national law, that telephone communications service providers retained traffic and location data of its users to prevent, detect, investigate and prosecute crime and safeguard the security of the State (par. 17).

The issue at hand was, similarly to the previous case, the tension between the fundamental right to privacy with regard to the processing of personal data *versus* the general interest of public security that the Directive intended to safeguard.

This exact same tension can be identified when we approach the topic of the usage of LFRTs. It is precisely due to the analogous nature of both judicial decisions, but

[112] ECtHR, Dudgeon v. the United Kingdom (Application no. 7525/76), 1981, paragraph 51.
[113] Facial Recognition Technology: Fundamental Rights Considerations In The Context Of Law Enforcement (2019), p. 22 [pdf] Publications Office of the European Union. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> [Accessed 25 September 2020].
[114] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014.

particularly the current one, that we have chosen to dissect it in further detail. We expect that this decision might shine a light on the legal stance of the EU regarding the technology we have been discussing.

Upon analysis, the Court asserted that the data being retained allowed very precise conclusions regarding the private life of the data subjects, notably their everyday life habits, permanent or temporary places of residence, social relationships, etc. (par. 27).

It follows that such data retention affected and interfered with private life and the rights guaranteed on article 7 of the Charter. Moreover, article 8 of the Charter was likewise touched upon and interfered with, as personal data was being processed with disregard to data protection requirements (pars. 29 to 37).

As the Advocate General poignantly points out "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance" (par. 37).

In its decision the Court noted that the limitation on fundamental rights and freedoms, notably article 7 and 8, must adhere to strict requirements (par. 38). These can be found under Article 52(1) of the Charter, which adds that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

On this point, the Court noted that while there was an interference with fundamental rights, the retention of data allowed by the Directive did not adversely affect the essence of those rights (pars. 39 and 40).

Regarding the requirement of general interest, the Court identified that the objective of public security was being genuinely satisfied, as the goal of the directive was to fight serious crime (pars. 41 to 44).

The issue arose when the Court observed the requirement of proportionality. It begun by recalling the settled case-law of the Court regarding the principle of proportionality, by which legislation must be appropriate to attain a legitimate objective and not exceed the limits of what is appropriate and necessary (par. 46). The question was then whether retention of data, as postulated in the directive, was appropriate to attain the objective of public security. The Court noted that such directive could be a valuable tool for criminal investigations and consequentially, that it could be considered an appropriate measure to attain the objective it pursued (par. 49).

Furthermore, as regards the necessity of the measure, it was conceded that the fight against serious crime was of the utmost importance, and such fight may depend on the usage of modern investigation techniques. Notwithstanding, the Court added that even a fundamental objective of general interest such as public security does not, in itself, justify the necessity of measures as the ones enacted by the data directive (par. 51).

When addressing whether the interference of the directive was limited to what was strictly necessary, the Court made reference to the fact that the directive impacted the privacy and data protection rights of practically the entire European population (par. 56). In essence, data was being processed in a generalised manner, not limited to a relevant geographical area or timeframe, and irrespective of whether the data subjects had a link with serious crime (pars. 57 to 59).

Moreover, the Court underscored that safeguards on fundamental rights and freedoms, such as conditions to access data and their subsequent use, or objective criteria for the period of data retention, were not in place. Consequentially, the interference with article 7 and 8 of the Charter was deemed to go beyond what was strictly necessary to attain the objective of the directive (pars. 60 to 65).

In conclusion, Directive 2006/24/EC failed the proportionality test of article 52 (1) of the Charter and was ruled invalid (pars. 69 to 73).

With this ruling the CJEU asserted its position in the conflict between the fundamental rights of EU citizens and the general interest of public security, steering away from a surveillance State stance.

As we have noted, it is not hard to find analogies between the ruling of the CJEU and the potential issues that the implementation of the technology we have been discussing can fall victim to. The ruling shines a light on the mistakes of the past, illuminating the road ahead, a road which LFRTs will most likely have to follow, if they are to be lawfully implemented in the EU.

2 – Secondary EU Law concerning LFRTs

After this analysis seen through the lens of fundamental rights, it is now time to move onto secondary European Law that can accommodate LFRTs. At first glance, as the technologies we are considering rely on the processing of special categories of personal data – biometric data – the adequate legislation to dissect would seem to be the GDPR.

The material scope of the GDPR is defined in article 2, which informs us that the Regulation does not apply (among others) when the processing of personal data is carried out by "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

This article excludes certain law enforcement activities from the material scope of the GDPR, thus if we are to look at LFRTs regulation from a law enforcement perspective, we need to seek a different legislative basis to rule over such activities.

Towards this end, we shall analyse the Data Protection Directive for Police and Criminal Justice Authorities (Directive 2016/680 of 27 April 2016), asserting the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

It is worth noting that the mentioned Directive complements the GDPR on the EU data protection legislation and for this reason they share a common ground of core principles and values. Nonetheless, it is important to explore them individually and the differences between them, ascertaining the reasoning for such differences and how LFRTs can find a legal ground on each of the legislative bodies.

2.1 – Implementing LFRTs under the General Data Protection Regulation

The GDPR, due to its Regulation status (Article 288 TFEU), has direct applicability and enforceability by law in all Member States.

The Regulation has the objective of strengthening an area of freedom, security and justice in the EU, promoting the well-being of natural persons, by setting rules on the processing of data that comply with their fundamental rights and freedoms, in particular the right to the protection of personal data (Recital 2 of the GDPR).

It builds on the foundations previously laid down by the Data Protection Directive, adding new and reinforced obligations, aiming to bring legal consistency and certainty to the EU on matters related to personal data processing (Recital 9). For this reason, Recital 10 of the GDPR reads that these rules shall be equivalent in all Member States, with "[c]onsistent and homogeneous application", notwithstanding the existence of a "margin of manoeuvre for Member States to specify its rules" on certain specific processing situations.

Article 2 of the GDPR asserts that the material scope of the regulation is the processing of personal data wholly or partly by automated means. Regarding LFRTs this can occur during the machine learning phase or when the technology is being deployed, for example, at schools, to verify student's attendance; at malls, to scan for known shoplifters; at the workplace, to monitor the clock-in and clock-out time of an employee; or even, as is becoming common place in China, to dispense toilet paper in public bathrooms[115].

For these scenarios to be a reality in the EU, the processing of facial images must be compliant with the principles relating to the processing of personal data asserted in article 5 of the GDPR.

This means that the processing of data when using LFRTs must follow these principles:

a) it must be lawful, fair and transparent in relation to the data subject;

b) the facial images must be collected for a specified, explicit and legitimate purpose and further processing must be compatible with those purposes (purpose limitation);

c) personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimisation);

d) data must be accurate and kept up to date (principle of data accuracy);

e) data must be stored for a reasonable period, that does not extend further than what is required for the purpose of facial recognition (principle of storage limitation);

f) must be processed in a manner that ensures personal data is safe from security breaches (principle of integrity and confidentiality);

g) the data controller (who determines the purposes and means of the processing of personal data) must be held accountable for compliance with the aforementioned principles (principle of accountability).

[115] [Unknown author] BBC News. 2017. Beijing Park Dispenses Loo Roll Using Facial Recognition. [online] Available at: <https://www.bbc.com/news/world-asia-china-39324431> [Accessed 25 September 2020].

While some of the principles are self-explanatory, it is pertinent to individually dissect some of them, understanding some of the practical issues they pose, when applied to LFRTs.

The following sub-chapters will explore some of these principles, further exploring how their effectiveness can contend with technologies of facial recognition.

In so far as they are relevant towards this dissertation, some articles of the GDPR will also be placed under scrutiny, as to provide us with a better understanding of the current EU legal framework and how it can shelter these technologies.

a) Principle of lawfulness

Article 6 of the GDPR lays down some requirements that confer lawfulness to the processing of personal data. However, as this dissertation delves into a special category of personal data, namely biometric data, the requirement of lawfulness shall be ascertained by analysing Article 9 of the GDPR which asserts the following:

"1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

This prohibition is not absolute, admitting exceptions under article 9 (2). It is worth noting, however, that two different moments of lawfulness of processing of data should be distinguished when we talk about LFRTs.

Firstly, we have the machine learning phase, that requires the machine to be given data (photographs) on which it can practice and learn. During this phase, lawfulness can be achieved through the exception of consent, under article 9, (2),

(a), by data subjects who consent on having their photographs used for the purpose of training a facial recognition technology.

Secondly, we have the actual deployment of the technology and the processing of personal data at large being crosschecked with a specific database of persons of interest.

Towards this end, consent can also be a valid legal basis. One practical example happened on the coastal town of Nice, which was the stage for testing of automated facial recognition systems in 2019, though its relationship with surveillance tech dates back to 2010[116]. The city has recently seen the deployment of around 2600 CCTV cameras[117] and became the first city in France to start trialling the technology[118] on a carnival event with about one thousand consenting adults. The trial, which was limited to the venue of the carnival, had the goal of testing different scenarios such as a lost child or elder, as well as the search for a person of interest. Whoever did not consent to be a volunteer on the trial had their faces blurred.

Likewise, in 2017 and 2018, the German government carried a trial of LFRTs on the Berlin Südkreuz railway station, with three hundred consenting adults who had their biometric data and names stored in a database, in exchange for a 25€ Amazon voucher[119].

[116] SCHNEIDER, Vanessa, 2014. A Nice, Souriez Vous Êtes Filmés. [online] Le Monde.fr. Available at: <https://www.lemonde.fr/municipales/article/2014/01/24/nice-souriez-vous-etes-filmes_4352555_1828682.html> [Accessed 25 September 2020].

[117] KAYALI, Laura, 2019. How Facial Recognition Is Taking Over A French City. [online] POLITICO. Available at: <https://www.politico.eu/article/how-facial-recognition-is-taking-over-a-french-riviera-city/> [Accessed 25 September 2020].

[118] Sciences et Avenir. 2019. Nice Teste Un Système De Reconnaissance Faciale Dans La Rue Pendant Le Carnaval. [online] Available at: <https://www.sciencesetavenir.fr/high-tech/data/la-ville-de-nice-teste-la-reconnaissance-faciale-dans-la-rue_131582> [Accessed 25 September 2020].

[119] DELCKER, Janosch, 2018. Big Brother In Berlin. [online] POLITICO. Available at: <https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/> [Accessed 25 September 2020].

One other relevant case, with a different outcome, is the one that occurred in Sweden – a country which in 1973 adopted the first data protection law in the world[120] – where a decision[121] from August 2019, held that the municipality of Skelleftea should be fined approximately 20 000 € for its use of LFRTs to monitor the attendance of students in a school.[122]

The pilot trial, that ran for over three weeks in Autumn of 2018, checked the attendance of one class composed of 22 students when they entered the classroom by capturing their biometric data and crosschecking it with an offline database. According to the Dean of the school Jörgen Malm, all the professors at that school combined spent a total of 17 000 hours per year in attendance reports. As he considered that the technology was "fairly safe" he decided to trial it[123].

Although consent was gathered from the parents and it was possible to refrain from the test at any time, the Swedish Data Protection Authority (DPA)[124] affirmed this was not enough to legally allow the collection of such personal data, as students had a legitimate expectation of privacy when entering a classroom.

The DPA found that the municipality had violated article 9, by processing biometric data to uniquely identify a natural person. Moreover, it considered that due to the significant inequality of the school-students relation, consent could not be used as a valid legal basis.

---

[120] ÖMAN, Sören, 2010. Implementing Data Protection in Law. [pdf] Stockholm: Stockholm Institute for Scandinavian Law, p.390. Available at: <https://www.scandinavianlaw.se/pdf/47-18.pdf> [Accessed 25 September 2020].

[121] 2020. Tillsyn Enligt EU:S Dataskyddsförordning 2016/679 – Ansiktsigenkänning För Närvarokontroll Av Elever. [pdf] Datainspektionen. Available at: <https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf> [Accessed 25 September 2020].

[122] Facial Recognition In School Renders Sweden's First GDPR Fine, 2019 [online] Available at: <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en> [Accessed 25 September 2020].

[123] VON HEIJNE, Thomas, 2019. Skolans Ovanliga Test: Elevernas Närvaro Registreras Med Kamerateknik. [online] SVT Nyheter. Available at: <https://www.svt.se/nyheter/lokalt/vasterbotten/skolans-ovanliga-test-registrerar-elevernas-narvaro-med-kamera> [Accessed 25 September 2020].

[124] Data Protection Authorities are independent supervisory bodies that each Member State shall provide, which are responsible for monitoring the application of the GDPR in the territory of said Member States, in accordance with article 51 of the same regulation.

This decision underscores that consent alone is not a blanket permission to data controllers. Moreover, Union or Member State law can assert that the data subject's consent is not sufficient to lift the general prohibition of the processing of certain personal data.

This is entrenched in (4) of the article 9 GDPR, which states that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of biometric data.

One other possible legal basis for the deployment of the technology lies in the exception listed in (2), (g), which states that the prohibition to the processing of special categories of data shall not apply when:

"(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

Following these coordinates, one could argue that indeed LFRTs can pursue an end-goal that is necessary for reasons of safeguarding fundamental rights and the interests of the data subject. As discussed in point 1.2 of the current chapter, one of the main arguments that is used to push for the implementation of this technology is crime prevention – this would result in a consequential increase on security and freedom of the general public, which, in principle, is aligned with the public interest.

Notwithstanding, following the case-law of the CJEU that we dissected when analysing the case of *Digital Rights Ireland*, public security in itself may not be sufficient to justify the usage of LFRTs.

The case for lawful processing of biometric data under the GDPR, becomes unsurprisingly less convoluted when it is used for purposes that stray away from the previously mentioned example – such as the case of monitoring students attendance – on such cases, the values of privacy and data protection easily overtake the convenience of having to manually check whether a student is present or not.

So far, the application of the technology has been done through trials on the basis of consent. However, it is worth pondering whether the GDPR would have sufficient elasticity to accommodate the actual deployment of the technology, considering its inherent issues, which will be showcased shortly in the next sections of this chapter.

As a last point, under the principle of lawfulness controllers and processors must not process personal data if doing so will in a general sense lead to an unlawful result. While using LFRTs, it is important to make sure these do not breach the lawfulness of extra-GDPR legislation, such as those governing privacy rights.

For this reason, the need to assess and correct algorithmic biases that result in false positives – which we have discussed in point 1.4 – must be addressed. If the principle of lawfulness is to be respected, the issue of intentionally or unintentionally discriminatory LFRTs cannot subsist. One of the paths to limit the existence of biases will be paved through adjustments, which will rely on a better clarification of the principle of data minimisation, as will be showcased on point d).

b) Principles of fairness and transparency

The principles of fairness and transparency are deeply tied. According to recital 60 of the GDPR, both principles require that data subjects must be informed about the existence of data processing and its purposes. Information should be provided at

various stages, as to allow a "re-balancing of the asymmetric data subject-controller relationship"[125] – this is likewise true for other tools given to data subjects under the GDPR, such as the power of consent.

This reversion to the *status quo ante*, helps us comprehend why the framework of the GDPR demands that data subjects are provided with concise, intelligible and easily accessible information regarding the identity of the controller as well as the purposes of the processing. Moreover, "[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing" (Recital 39).

To aid our understanding of how these principles can be practically applied to LFRTs, the European Data Protection Board (EDPB) has released some guidelines regarding the usage of video surveillance[126], wherein the independent European body has suggested a multi-layered approach to preserve the principle of transparency.

The first layer should be composed of a warning sign, at a reasonable distance of the monitored area, which may be used in combination with an icon "in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing" (article 12, (7)).

The sign should likewise respect the right to information of article 13 (e.g. containing the identity and contact details of the controller and the purposes of the processing).

The second layer of information should be clearly referred by the warning sign, for example by redirecting the data subject to an information desk or reception, or

[125] CLIFFORD, Damian and AUSLOOS, Jef, 2017, Data Protection and the Role of Fairness [online]. KU Leuven Centre for IT & IP Law. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139, p. 5 [Accessed 25 September 2020].
[126] 2019. Guidelines 3/2019 On Processing of Personal Data Through Video Devices. [pdf] European Data Protection Board, pp.21, 22 and 23. Available at: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf> [Accessed 25 September 2020].

by means of a QR code, in so far as accessing this second layer of information can be done without entering the surveyed area.

On this point it should be underscored that the right to information, when automated decision-making is concerned – which is the case regarding LFRTs – requires the data controller to provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (article 13, (1), (f) and article 14, (2), (g) GDPR).

While on paper this article seems to offer a reasonable solution, the fact of the matter is that machine learning leads to the already mentioned "black box effect" (see point 1.4). This self-learning phase is particularly complicated to decipher even to the original data scientists or programmers; thus, it sometimes becomes impractical to explain AI decision-making[127].

To counteract the black box issue, Explainable AI (XAI) has since been introduced to the machine learning field, lifting the veil of apparently abstract algorithmic decisions of AI.[128] XAI aims to explain why an AI system comes up with a certain solution or decision, it is an approach to AI that seeks to analyse the learning process. This has the double effect of allowing users to see what is going on under the "hood" of the software – thus bolstering fairness and transparency – but also helps the software developer to find and address issues that can negatively affect the learning phase.

c) Principle of purpose limitation

This principle imposes that data can only be collected for specified, explicit and legitimate purposes and that "[t]he processing of personal data for purposes other

[127] ROUSE, Margaret, 2019. What Is Black Box AI? - Definition from Whatis.Com. [online] WhatIs.com. Available at: <https://whatis.techtarget.com/definition/black-box-AI> [Accessed 25 September 2020].
[128] SCHMELZER, Ron, 2019. Understanding Explainable AI. [online] Forbes. Available at: <https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/#d158a267c9ef> [Accessed 25 September 2020].

than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected" (Recital 50).

This means that if a data controller used personal data with the purpose of training a LFRT software through machine learning, it cannot alter this data's purpose to have those photographs being part of a facial recognition database, when the technology is already deployed. This would require a separate ground for processing data (e.g. consent), not doing so would negatively impact the reasonable expectations of data subjects.

According to the decision of the Swedish DPA that we mentioned earlier, the municipality had violated not only article 9, regarding the lawfulness of the trial of LFRTs, but also article 5, especially for violating the principle of purpose limitation and data minimisation principle. According to the decision, the pupils' personal data was processed in a more intrusive way than what was necessary for the stated purpose (attendance check).

d) Principle of data minimisation

In consonance with the case-law we have previously explored, even if LFRTs are deployed lawfully, they must be used in a way that respects the principle of proportionality to attain the aim pursued. The usage of LFRTs must stem from a "pressing social need"[129], achieving a legitimate goal that would not be possible to achieve through less onerous means.

Data minimisation requires that processing of data is limited to what is adequate, relevant and necessary in relation to the legitimate purposes it seeks to achieve.

[129] ECtHR, Dudgeon v. the United Kingdom (Application no. 7525/76), 1981, paragraph 51.

This means that processing of data must comply with a proportionality test, through which the specified, explicit and legitimate purpose that the processing of data is trying to achieve cannot be reasonably fulfilled through less intrusive means, i.e. means that are less interfering with fundamental rights and interests of data subjects – this test was failed on the aforementioned Swedish case.

Once more it is important to individually consider the pre-deployment phase of LFRTs, namely the machine learning phase.

During this phase, respecting the principle of data minimisation means that such data must be **adequate** in relation to the purpose it seeks to achieve – identifying facial features and matching them with a facial image in a database. For this purpose, the system must be trained using a wide variety of data that should represent people from different age groups, genders, ethnicities and races; but also, that data should be of good quality, i.e. good resolution photos, frontal pictures fully displaying facial features.

The non-compliance with this requisite is one of the main culprits of unintended discriminatory biases in LFRTs mentioned in point 1.4 – most facial recognition algorithms being developed in the West were trained using predominantly white men[130]. The result is that these technologies excel at identifying white males, but lack the same quality, for example, when it comes to black women.

This means that LFRTs must be trained using a significant amount of personal data in order to achieve an acceptable accuracy-rate, which might seem counterintuitive, considering this is a principle that claims for the "minimisation" of data. Notwithstanding, it is worth recalling that these principles do not operate in a vacuum, but rather are in concurrent motion with other principles, such as that

[130] 2019. *Facial Recognition Technology: Fundamental Rights Considerations in The Context of Law Enforcement*, p. 27 [pdf] Publications Office of the European Union. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> [Accessed 25 September 2020].

of fairness or accuracy[131], as well as fundamental rights (article 1, (2)), such as the right to not be discriminated against (article 21 of the Charter).

The second requisite for personal data under this principle is that of **relevancy**. For the purposes of training LFRTs, the pertinent personal data should, in principle, be photographs only. This means that there is no need to have the full name or data of birth of the data subject to which the photograph belongs to.

Thirdly, personal data must be **limited** to what is necessary. What this entails is that data controllers should be able to identify how much data they will need to achieve the necessary level of accuracy in their LFRTs. This raises the question: what is the necessary accuracy that technologies of facial recognition must achieve in order to be lawfully deployed? Knowing well that having a system with a 100% accuracy rate is idyllic, it is worth pondering what policymakers in the EU will consider as "necessary" for the deployment of the technology. This will of course depend on the purpose towards which the technology is to be used and the rights and freedoms at stake – if, for example, it is used to combat serious crime, the fail-rate requirement of the software has to be significantly lower than if, for example, the technology is used for marketing purposes.

Regarding the actual deployment phase of the technology, it is worthwhile to consider a practical case in the French region of Provence-Alpes-Côte d'Azur, namely in Nice and Marseille, where the push for LFRTs has expanded the technology to the entrance of two schools located therein. On the 29th of October 2019, the *Commission nationale de l'informatique et des libertés (CNIL)*, the French data protection regulatory authority, did an impact assessment and held that

[131] BIEGA, Asia, et al. Operationalizing the Legal Principle of Data Minimization for Personalization. arXiv preprint arXiv:2005.13718, 2020, p. 2.

the proposed technology was against the GDPR's principles of proportionality and data minimisation[132]. It considered that the intended objectives could be attained through less intrusive measures, as biometric data processing is particularly sensitive, justifying a bigger protection of individuals. Furthermore, the regulatory body claimed that facial recognition systems are especially intrusive, displaying a great risk on individual freedoms of the citizens involved, even more so when these are minors.

From the combined decisions of the Swedish and French DPA we can observe that the principle of data minimisation is a strong argument against LFRTs, as in many instances there will be a less intrusive manner to carry out the purpose that such technologies entail.

e) Principle of data security

Concerning the security of personal data, article 32 lists the appropriate technical and organisational measures that the controller and the processor must implement, in order to ensure the security of processing of personal data. In that article we can find, amongst others, the encryption of data and resilience of processing systems. Nonetheless, it is of the utmost importance to readdress a vulnerability of the security of personal data, previously explored on chapter IV, point 2.2 – the EU does not have adequate data infrastructures to store the amounts of data it seeks to benefit from. This is especially relevant in data-heavy technologies such as facial recognition.

While the data strategy released in 2020 aims to solve this issue, as of today, the EU is dependent on data storage infrastructures located in the US or China. As Benjamin Strasser, a member of the German Parliament asserts: "It's like with

[132] Cnil.fr. 2019. Expérimentation De La Reconnaissance Faciale Dans Deux Lycées: La CNIL Précise Sa Position. [online] Available at: <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position> [Accessed 25 September 2020].

access to gas — if we make our entire energy supply rely on a few nations in the world who get to control access, we're becoming politically dependent. (…) It's no different when it comes to data and data services."[133]

This led Germany's lawmakers and industrial leaders to push for a European Data storage infrastructure – a project which has since been named "Gaia-X" – to counter the increasing dependence on storage of sensitive data on foreign servers, which is effectively making Europe's claim towards technological sovereignty a farfetched dream.

A practical example of this dependency can be seen in the German Federal police, whose bodycam footage is being stored on the cloud servers of US Tech Giant Amazon. This obviously raises concerns for the topic of facial recognition systems – even more so when the area concerned is law enforcement. If databases and the data that is processed during the deployment of the technology has to be stored outside of the EU, this infrastructural dependence can lead to serious breaches of privacy for EU citizens.

On this point, and counteracting such fears of privacy breaches, in July of 2020 there was a CJEU decision on the case known as *Schrems II*[134]. The decision concerned the transatlantic transfer of personal data between the US and the EU, namely the non-compliance with the EU standards of privacy and data protection. The framework under which these transfers occurred, known as the EU-US Privacy Shield, in principle guaranteed that privacy and data protection rights exported from the EU to the US were processed in compliance with EU laws and principles. Nonetheless, the Court found that the Privacy Shield Decision could not ensure a level of protection essentially equivalent to that arising from the Charter (par. 181). As an example, under the Decision's paragraph I.5. of Annex II, adherence to EU principles was limited "to the extent necessary to meet national

[133] DELCKER, Janosch, 2019. Germany's Plan to Control Its Own Data. [online] POLITICO. Available at: <https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/> [Accessed 25 September 2020].
[134] CJEU Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 2020.

security, public interest, or law enforcement requirements". This derogation, as the Court found, enabled interference on EU citizens' fundamental rights, based on national security and public interest requirements or on domestic legislation of the US (pars. 164 and 165).

Such incompatibility led the CJEU to declare the Privacy Shield Decision invalid (par. 201).

This decision leaves the door open towards the construction of a legal framework that does not forsake the security and legitimate expectations of European data subjects.

f) Automated Processing

Now that we have delved into some of the core principles of the GDPR, it is now time to move onto other articles that will prove useful in our task of understanding the legal framework that accommodates LFRTs. One such article is Article 22, which covers the rights of data subjects regarding automated individual decision-making. Therein, it can be read that "data subjects shall have the right not to be subject to a decision based solely on automated processing, (…) which produces legal effects concerning him or her or significantly affects him or her".

Naturally, when it comes to LFRTs, the processing of personal data is bound to occur via automated means – a camera captures a facial image that is processed through a facial recognition software which attributes that image to a person in the software's database. This automation can pose some dangers to the safety of personal data, hence the article's general prohibition on fully automated decisions.

This however allows exceptions, even when special categories of personal data are concerned, namely if article 9(2), point (a) or (g) apply – so far as authorised by Union or Member-State Law and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are put in place (article 22, (4)). One

such safeguard is the right to obtain human intervention to mitigate the decision-making process.

Regarding this subject, it is worth recalling that human intervention is not without its own vicissitudes, as displayed previously in point 2 of chapter III or point 1.4 of this chapter.

g) Data protection impact assessment and prior consultation

Previously we saw that the decision of the Swedish DPA, regarding the high school using LFRTs to check for student's attendance, held that article 5 and 9 of the GDPR had been violated. The third and last articles the supervisory authority claimed the municipality of Skelleftea had violated were article 35 and 36 – respectively, the lack of a data protection impact assessment and prior consultation, when implementing the technology.

Article 35 requires that a type of processing that uses new technologies, which are likely to result in a high risk to the rights and freedoms of natural persons, shall be preceded by a data protection impact assessment carried out by the data controller.

In the case we have been analysing, the school, resorting to new technologies, did not "carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". According to the DPA, the school board did conduct a risk assessment, but not a data protection impact assessment, that verified whether data subjects' rights and freedoms would be at risk, neither if the intended measures of processing were proportionate.

It follows that article 35, (3), (b) imposes that a data protection impact assessment is required, in particular whenever special categories of data are processed – which will always be the case when processing data in LFRTs.

As a direct consequence of the lack of a data protection impact assessment, the DPA considered there had been a violation of article 36, as the school did not consult the supervisory authority.

2.2 – Implementing LFRT under the Data Protection Directive for Police and Criminal Justice Authorities

First and foremost, the legal instrument we will now analyse complements the GDPR, having the clear distinction that the latter is a regulation, while the former is a directive. Such entails that it only goes as far as to define the aims, requirements and concrete end-results that every Member State must achieve through the transposition of such directive to their domestic law.

The Law Enforcement Directive, due to its legal nature, leaves the Member States with a bigger margin of discretion that can, much like what happened with the Data Protection Directive of 1995, contend with the goal of harmonising data protection rules across the board of the EU. However, this level of flexibility is necessary in the law enforcement endeavour, as we will soon illustrate.

The Law Enforcement Directive came into force to fill a legislative void regarding the processing of personal data by law enforcement authorities, a sector not regulated by the Data Protection Directive. As it entered into force, it repealed the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Article 1 of the directive lays down the subject-matter and objectives of the directive, which is the protection of fundamental rights and freedoms, in particular the personal data of individuals, when their data is processed in the context of law enforcement activities (e.g. prevention of criminal offences and of threats to public security).

Naturally, due to the complementary aspect of this directive regarding the GDPR, the former is similar in nature to the Regulation. There are however some relevant differences which are worth our time to explore, so that we can understand how LFRTs must comply with different data protection requisites.

a) Data protection principles under the Law Enforcement Directive

Firstly, it is relevant to explore the core principles of this directive which are asserted in article 4. While most principles are postulated as they are in the GDPR, the article denotes some small but relevant differences when compared to article 5 of the Regulation:

a) The principle of lawfulness and fairness is affirmed, but not the principle of transparency. Regarding the principle of lawfulness, article 8 upholds that processing shall be lawful "only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority" for the purposes of the directive laid down on article 1. This is significantly different from the GDPR's lawfulness, which can be based on six legal grounds;
b) The principle of purpose limitation is less strict, allowing the data controller to process personal data for purposes other than the initial one. This possibility needs to meet two requirements: 1) the controller is authorised to process such personal data by Union or Member State Law; and 2) processing is necessary and proportionate to that other purpose in accordance with Union or Member State Law (article 4, (2))
c) Data minimisation is worded with a subtle difference. While in the GDPR personal data must be "adequate, relevant and **limited to what is necessary**", on this legal instrument personal data must be "adequate, relevant and **not excessive in relation to the purposes for which they are processed**". This confers law enforcement authorities slightly more leeway when it comes to going past the data minimisation principle.
d) Regarding the time-limit for storage and review of personal data, the appropriate time limit for law enforcement to erase data is defined by the Member State implementing the Directive, as postulated in article 5 of the LED.

This denotes that some of the directive's principles are conceded a higher level of flexibility in comparison with the GDPR. This flexibility can be understood if we consider the special nature of law enforcement.

As an example, if the principle of transparency existed as it does in the GDPR, it could contend with the end-goal of a criminal investigation. Therefore, it is no surprise that the suspect of a crime does not enjoy the same level of rights regarding information of personal data processed under the scope of this directive, as those that he would enjoy if his data was being processed under the material scope of the GDPR. This does not preclude the data subject from being conceded some information rights, as is clear from article 13, in so far as this does not contend with the objective of the directive.

The same reason justifies why the principle of storage limitation has a higher level of flexibility – as "[t]he information collected and stored by competent authorities for a particular case may be found extremely useful in resolving future cases."[135]

b) Categories of data subjects

Article 6 specifies different categories of data subjects. As the European Union Agency for Fundamental Rights asserts, watchlists allow for the "assessment of the real purpose, necessity and social need for employing live facial recognition technology"[136], therefore, clarifying this point is an essential way forward for the regulation of LFRTs. This is of the utmost importance, as these categories will come into play on the application of LFRTs in the context of law enforcement activities.

[135] BOILLAT, Philippe; KJAERUM, Morten. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, 2014, p. 283.

[136] 2019. *Facial Recognition Technology: Fundamental Rights Considerations in The Context Of Law Enforcement*, p. 11 [pdf] Publications Office of the European Union. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> [Accessed 25 September 2020].

This was likewise manifested in 2018 by the German government, after the test in 2017 and 2018, on the train station Südkreuz with the objective of identifying and tracing criminals and terrorists.

In September 2018, the police released the results of the test[137]. Therein, it was stated that a legislation on LFRTs is needed, as to solve, among others, the issue of who to include in facial recognition watchlists (e.g. terrorists, sexual offenders, missing children).

This preface explains why article 6 is a valuable legal basis, but one that needs further specification, for the implementation of LFRTs. It displays the following:

"Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence;

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b)."

[137] 2018. Biometrische Gesichtserkennung. [pdf] Potsdam: Bundespolizeipräsidium Potsdam. Available at: <https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile> [Accessed 25 September 2020].

It is imperative that the data subjects that can be monitored through LFRTs are further specified (perhaps in a separate legislative instrument). The reasoning for this lies in the intrusive nature of the technology and its potential to contend with privacy and data protection rights. Therefore, a blanket permission that allows monitoring through LFRTs of any "(b) persons convicted of a criminal offence" is too generic, as it can encompass a wide range of crimes that vary in seriousness.

c) Processing of special categories of personal data

Regarding provisions on processing of special categories of data (such as biometric data), article 10 asserts that the processing of special categories of personal data "(…) shall be allowed **only where strictly necessary**, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject."

While article 9 of the GDPR offers a generally prohibitive first paragraph and then goes on to list *ten* exceptions to the prohibition, contrary to the trend so far, article 10 of this directive is more rigid, contemplating *three* non-cumulative conditions, subject to appropriate safeguards. This is the formal recognition that special categories of data are a delicate area that demands stricter rules, especially when being processed by law enforcement authorities.

d) Automated individual decision-making

Article 11 covers automated individual decision-making and does not diverge from the solution found on the GDPR, allowing decisions based on special categories of

data to occur, as long as suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

e) Data Protection Impact Assessment

Lastly, and in parallel to the requirement laid down in article 35 of the GDPR, given the sensitive area of law enforcement and the degree to which it can influence rights and freedoms of natural persons it is necessary to ascertain the impact of LFRTs on such values. Therefore, under article 27 of the LED, and since this technology is indubitably of high risk, its application will always have to be preceded by a data protection impact assessment.

VI – CONCLUDING NOTES

Throughout this dissertation we analysed the potential accommodation of Live Facial Recognition Technologies in the current legal and political paradigm of the European Union.

While it is not unfathomable to implement LFRTs under the GDPR or the Law Enforcement Directive, it is hard to ignore some of the shortcomings of the technology and the potential risks it poses on fundamental rights and freedoms.

In the decisions we made reference to, the common denominator seems to be the failure of the proportionality test when contraposing the general interest of public security *versus* the enjoyment of the right to privacy and data protection.

It is worth pondering if the answer will be different once these technologies acquire more technical robustness. But even then, if mismatches or discriminatory results that prejudice minorities are reduced and LFRTs reach a state of near technical perfection, we must address whether we are ready to face the societal changes that such technology will force upon us.

As illustrated, this technology can contribute towards a greater dilution between what is public and private. In doing so, it can have a direct impact on democratic society as we know it, as the chilling effect caused by constant surveillance can lead to the apparent inexistence of political opposition.

On the other end of the spectrum, it may lead to an increased safety of the population at large, as it could be used to find missing children or elderly, or fight serious crime.

These considerations must not be dismissed when adopting new legislation on these matters. The legislative solution the EU will enact, will ideally define an acceptable accuracy rate for the lawful deployment of LFRTs, clearly assert which data subjects can be monitored under law enforcement activities and address the issues of human oversight we mentioned.

It is of the utmost importance that the technology's implementation and operation is within a well-established legal framework, one that is wary of politically motivated surveillance.

In the end, and to the extent that such is a possibility, a clear balance must be struck between the fundamental rights of EU citizens and the general public interest. If done properly, we will hopefully reach the destination of trustworthy European live facial recognition technologies.

BIBLIOGRAPHY

1 – Books and articles

BIEGA, Asia, et al. Operationalizing the Legal Principle of Data Minimization for Personalization. arXiv preprint arXiv:2005.13718, 2020.

BOILLAT, Philippe; KJAERUM, Morten. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, 2014.

CITRON, Danielle Keats, 2007. "Technological due process." Wash. UL Rev. 85.

CLIFFORD, Damian and AUSLOOS, Jef, 2017, Data Protection and the Role of Fairness [online]. KU Leuven Centre for IT & IP Law. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139. [Accessed 25 September 2020].

GATES, Kelly A. Our biometric future: Facial recognition technology and the culture of surveillance. NYU Press, 2011.

GILL, Pat. Technostalgia: Making the future past perfect. Camera Obscura: Feminism, Culture, and Media Studies, 1997.

HARTZOG, Woodrow; SELINGER, Evan. Surveillance as loss of obscurity. Wash. & Lee L. Rev., 2015, 72.

HOFFMAN, David, BRUENING, Paula, and CARTER, Sophia. "The right to obscurity: How we can implement the Google Spain decision." NCJL & Tech. 17 (2015).

HSU, Hwai-Jung and CHEN, Kuan-Ta, 2015. Face Recognition on Drones. [pdf] Institute of Information Science, Academia Sinica. Available at: <https://www.researchgate.net/publication/300655333_Face_Recognition_on_Drones> [Accessed 25 September 2020].

INTRONA, Lucas, and WOOD, David. "Picturing algorithmic surveillance: The politics of facial recognition systems." Surveillance & Society 2.2/3 (2004).

LAZAR, Seth, BENN, Claire and GÜNTHER, Mario, 2020, Large-scale facial recognition is incompatible with a free society. The Conversation [online]. 2020. Available from: https://theconversation.com/large-scale-facial-recognition-is-incompatible-with-a-free-society-126282 [Accessed 25 September 2020].

MCCRUDDEN, Christopher. Human dignity and judicial interpretation of human rights. European Journal of international Law, 2008, 19.4.

NILSSON, Nils J., Principles of artificial intelligence. Morgan Kaufmann, 2014.

ÖMAN, Sören, 2010. Implementing Data Protection in Law. [pdf] Stockholm: Stockholm Institute for Scandinavian Law. Available at: <https://www.scandinavianlaw.se/pdf/47-18.pdf> [Accessed 25 September 2020].

OOSTVEEN, Manon; IRION, Kristina. The golden age of personal data: How to regulate an enabling fundamental right? In: Personal Data in Competition, Consumer Protection and Intellectual Property Law. Springer, Berlin, Heidelberg, 2018.

ORWELL, George. “1984”, Penguin Books, London, (first published in 1949), 2008.

RAO, Varuna. Face Recognition: Is It a Match? Oklahoma Academy of Science Publication, 2009.

ROBERTS, Jessica L. Protecting Privacy to Prevent Discrimination. Wm. & Mary L. Rev., 2014, 56.

SELINGER, Evan; HARTZOG, Woodrow. Why you have the right to obscurity. Christian Science Monitor (Apr. 15, 2015), 2015.

SOLOVE, Daniel, The digital person: Technology and privacy in the information age. NyU Press, 2004.

TOOM, Viktor, 2018. Cross-Border Exchange and Comparison of Forensic DNA Data in The Context of The Prüm Decision. [pdf] European Parliament's Committee on Civil Liberties, Justice and Home Affairs. Available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf,> [Accessed 8 September 2020].

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, 1890.

2 – Jurisprudence

CJEU, Case C-145/09 Land Baden-Württemberg v Panagiotis Tsakouridis, 2010.

CJEU, Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 2020.

CJEU, Google Spain v. AEPD, 2014. Available at: <http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065/> [Accessed 25 September 2020].

CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014.

CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010.

COURT OF APPEAL (CIVIL DIVISION), R (Bridges) v Chief Constable of the South Wales Police, 2020 Available at: <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> [Accessed 25 September 2020].

ECtHR, Dudgeon v. the United Kingdom (Application no. 7525/76), 1981.

ECtHR, López Ribalda and Others v. Spain, 2019.

ECtHR, Peck v. the United Kingdom, 2003.

ECtHR, S. and Marper v. the United Kingdom (30562/04 and 30566/04), 2008.

ECtHR, Tysiac v Poland (case 5410/03), 2007.

HIGH COURT OF JUSTICE QUEEN'S BENCH DIVISION DIVISIONAL COURT SITTING AT CARDIFF CIVIL JUSTICE CENTRE, R (Bridges) v Chief Constable of the South Wales Police, 2019. Judiciary.uk. Available at: <https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf> [Accessed 25 September 2020].

Tribunal de Justiça do Estado de São Paulo, Processo Nº: 1090663-42.2018.8.26.0100, 2018. Available at: <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/sp_10906634220188260100_14092018.pdf?fbclid=IwAR2kS-QU8Fm5bNOpbijV6TncqsL6E1ru1XvKQtomBdFc7Zqo_nsNpyFtjh8> [Accessed 25 September 2020].

3 – News Articles

BBC News. 2017. Beijing Park Dispenses Loo Roll Using Facial Recognition. [online] Available at: <https://www.bbc.com/news/world-asia-china-39324431> [Accessed 25 September 2020].

BBC News. 2020. Facial Recognition: EU Considers Ban of up to Five Years. [online] Available at: <https://www.bbc.com/news/technology-51148501> [Accessed 25 September 2020].

BBC News. 2020. IBM Abandons 'Biased' Facial Recognition Tech. [online] Available at: <https://www.bbc.com/news/technology-52978191> [Accessed 8 September 2020].

BOSELLI, André, 2020. Polícia Paulista Usará Reconhecimento Facial Em Investigações. [online] Consultor Jurídico. Available at:

<https://www.conjur.com.br/2020-jan-29/policia-paulista-usara-reconhecimento-facial-investigacoes> [Accessed 25 September 2020].

BUCKLEY, Chris; MOZUR, Paul; RAMZY, Austin. How China turned a city into a prison: A surveillance state reaches new heights. The New York Times, [online] 2019, Available at: <https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html> [Accessed 25 September 2020].

CAMPBELL, Charlie. How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens. time. com/collection/davos-2019/5502592/china-social-credit-score, [online] 2019, Available at: <https://time.com/collection/davos-2019/5502592/china-social-credit-score/> [Accessed 25 September 2020].

CAMPBELL, Zach and JONES, Chris, 2020. Leaked Reports Show EU Police Are Planning A Pan-European Network of Facial Recognition Databases. [online] The Intercept. Available at: <https://theintercept.com/2020/02/21/eu-facial-recognition-database/> [Accessed 25 September 2020].

Cnil.fr. 2019. Expérimentation De La Reconnaissance Faciale Dans Deux Lycées: La CNIL Précise Sa Position. [online] Available at: <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position> [Accessed 25 September 2020].

COWAN, Jill, 2019. San Francisco Banned Facial Recognition. Will California Follow? [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/07/01/us/facial-recognition-san-francisco.html> [Accessed 25 September 2020].

CRUZ, Elaine Patricia, 2020. Polícia Usa Sistema De Reconhecimento Facial No Carnaval De São Paulo. [online] Agência Brasil. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-02/policia-usa-sistema-de-reconhecimento-facial-no-carnaval-de-sao-paulo> [Accessed 25 September 2020].

DELCKER, Janosch, 2018. Big Brother in Berlin. [online] POLITICO. Available at: <https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/> [Accessed 25 September 2020].

DELCKER, Janosch, 2019. Europe's Silver Bullet in Global AI Battle: Ethics. [online] POLITICO. Available at: <https://www.politico.eu/article/europe-silver-bullet-global-ai-battle-ethics/> [Accessed 25 September 2020].

DEMARTINI, Felipe, 2018. Justiça Ordena Fim De Coleta De Dados Faciais Na Linha Amarela Do Metrô De SP. [online] Canaltech. Available at: <https://canaltech.com.br/seguranca/justica-ordena-fim-de-coleta-de-dados-faciais-na-linha-amarela-do-metro-de-sp-122744/> [Accessed 25 September 2020].

EDRi. 2019. Danish DPA Approves Automated Facial Recognition. [online] Available at: <https://edri.org/danish-dpa-approves-automated-facial-recognition/> [Accessed 25 September 2020].

Folha de S. Paulo. 2020. Polícia Prende 413 Pessoas No 1º Fim De Semana Oficial Do Carnaval De Rua Em SP. [online] Available at: <https://www1.folha.uol.com.br/cotidiano/2020/02/policia-prende-413-pessoas-no-1o-fim-de-semana-oficial-do-carnaval-de-rua-em-sp.shtml> [Accessed 25 September 2020].

GERSHGORN, Dave, 2020. Exclusive: Live Facial Recognition Is Coming to U.S. Police Body Cameras. [online] Medium. Available at: <https://onezero.medium.com/exclusive-live-facial-recognition-is-coming-to-u-s-police-body-cameras-bc9036918ae0> [Accessed 25 September 2020].

HAINS, Tim, 2019. Protesters in Hong Kong Tear Down Facial Recognition Towers as Violence Escalates. [online] Realclearpolitics.com. Available at: <https://www.realclearpolitics.com/video/2019/08/25/protesters_in_hong_kong_tear_down_facial_recognition_towers_as_violence_escalates.html> [Accessed 25 September 2020].

KAYALI, Laura, 2019. How Facial Recognition Is Taking Over A French City. [online] POLITICO. Available at: <https://www.politico.eu/article/how-facial-recognition-is-taking-over-a-french-riviera-city/> [Accessed 25 September 2020].

LEE, Dave, 2019. San Francisco Is First US City to Ban Facial Recognition. [online] BBC News. Available at: <https://www.bbc.com/news/technology-48276660> [Accessed 25 September 2020].

MANANCOURT, Vincent, 2020. Controversial US Facial Recognition Technology Likely Illegal, EU Body Says. [online] POLITICO. Available at: <https://www.politico.eu/article/clearview-ai-use-likely-illegal-says-eu-data-protection-watchdog/> [Accessed 25 September 2020].

MARR, Bernard, 2019, Facial Recognition Technology: Here Are the Important Pros and Cons. Forbes [online]. 2019. Available from: <https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#61deecf714d1/> [Accessed 25 September 2020].

MOZUR, Paul, 2019. In Hong Kong Protests, Faces Become Weapons. [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html> [Accessed 25 September 2020].

MOZUR, Paul, 2019. One Month, 500,000 Face Scans: How China Is Using A.I. To Profile A Minority. [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> [Accessed 7 September 2020].

O'SULLIVAN, Donnie. This man says he's stockpiling billions of our photos'. CNN Business, February 2020, 10. Available at: < https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html> [Accessed 25 September 2020].

OKUMURA, Renata, 2020. Carnaval De SP Terá Drones, Reconhecimento Facial E 15 Mil Policiais Por Dia. [online] Estadão. Available at: <https://sao-

paulo.estadao.com.br/noticias/geral,carnaval-de-sp-tera-drones-reconhecimento-facial-e-15-mil-policiais-por-dia,70003197829> [Accessed 25 September 2020].

SCHMELZER, Ron, 2019. Understanding Explainable AI. [online] Forbes. Available at: <https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/#d158a267c9ef> [Accessed 25 September 2020].

SCHNEIDER, Vanessa, 2014. A Nice, Souriez Vous Êtes Filmés. [online] Le Monde.fr. Available at: <https://www.lemonde.fr/municipales/article/2014/01/24/nice-souriez-vous-etes-filmes_4352555_1828682.html> [Accessed 25 September 2020].

SCHUPPE, Jon, 2019. Should Police Body Cameras Have Facial Recognition Tech? Axon, The Largest U.S. Maker of Devices, Says No. [online] NBC News. Available at: <https://www.nbcnews.com/news/us-news/should-police-body-cameras-have-facial-recognition-tech-axon-largest-n1023271> [Accessed 25 September 2020].

Sciences et Avenir. 2019. Nice Teste Un Système De Reconnaissance Faciale Dans La Rue Pendant Le Carnaval. [online] Available at: <https://www.sciencesetavenir.fr/high-tech/data/la-ville-de-nice-teste-la-reconnaissance-faciale-dans-la-rue_131582> [Accessed 25 September 2020].

STOLTON, Samuel, 2020. After Clearview AI Scandal, Commission 'In Close Contact' With EU Data Authorities. [online] www.euractiv.com. Available at: <https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/> [Accessed 25 September 2020].

STOLTON, Samuel, 2020. EU Police Plan Massive Facial Recognition Database. [online] www.euractiv.com. Available at: <https://www.euractiv.com/section/digital/news/eu-police-plan-massive-facial-recognition-database/> [Accessed 8 September 2020.]

VALENTINO-DEVRIES, Jennifer, 2020. How the Police Use Facial Recognition, And Where It Falls Short. [online] Nytimes.com. Available at: <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html> [Accessed 25 September 2020].

VON HEIJNE, Thomas, 2019. Skolans Ovanliga Test: Elevernas Närvaro Registreras Med Kamerateknik. [online] SVT Nyheter. Available at: <https://www.svt.se/nyheter/lokalt/vasterbotten/skolans-ovanliga-test-registrerar-elevernas-narvaro-med-kamera> [Accessed 25 September 2020].

WOOD, Charlie, 2020. Leaked Documents Reportedly Show Clearview AI Tech Was Used by Walmart And Many Private Firms — Contradicting Its Claims It Only Works with Law Enforcement. [online] Business Insider. Available at: <https://www.businessinsider.com/clearview-ai-reportedly-sold-tech-to-fbi-other-enfocrement-agencies-2020-2> [Accessed 25September 2020].

4 – Others

A European Strategy for Data. [pdf] Brussels: European Commission, 2020. Available at: <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> [Accessed 25 September 2020].

ACTON, Lord. Letter to Bishop Mandell Creighton. Retrieved on June 1887, 29: 2009.

ALA-PIETILÄ, Pekka, 2019. Towards Trustworthy AI - Ethics & Competitiveness Go Hand-In-Hand. [online] Available at: <https://ec.europa.eu/digital-single-market/en/blogposts/towards-trustworthy-ai-ethics-competitiveness-go-hand-hand> [Accessed 25 September 2020].

Artificial Intelligence High-Level Expert Group, Ethics Guidelines for Trustworthy AI, 2019 [online] PDF available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation> [Accessed 25 September 2020].

Biometrische Gesichtserkennung. [pdf] Potsdam: Bundespolizeipräsidium Potsdam, 2018 Available at: <https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile> [Accessed 25 September 2020].

COM (2018) 237 final. Artificial Intelligence for Europe. [pdf] Brussels: European Commission, 2018. Available at: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF> [Accessed 25 September 2020].

Europarl.europa.eu. 2020. Answer for Question E-000383/20 [online] 2020. Available at: <https://www.europarl.europa.eu/doceo/document/E-9-2020-000383-ASW_EN.html> [Accessed 25 September 2020].

European Commission, 2020. Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence. [online] Available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273> [Accessed 25 September 2020].

Facial Recognition in School Renders Sweden's First GDPR Fine, 2019 [online] Available at: <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en> [Accessed 25 September 2020].

Facial Recognition Technology: Fundamental Rights Considerations in The Context of Law Enforcement (2019), [pdf] Publications Office of the European Union. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> [Accessed 25 September 2020].

Facial Recognition Technology: Fundamental Rights Considerations in The Context of Law Enforcement, [pdf] Publications Office of the European Union, 2019. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-

facial-recognition-technology-focus-paper-1_en.pdf> [Accessed 25 September 2020].

Fines and Facial Recognition - BBC Click. 2019. [video] London, U.K.: BBC. Available at: <https://www.youtube.com/watch?v=0oJqJkfTdAg/> [Accessed 25 September 2020].

GOV.UK. n.d. Review of Public Sector Equality Duty. [online] Available at: <https://www.gov.uk/government/groups/review-of-public-sector-equality-duty-steering-group> [Accessed 25 September 2020].

GREEN, Ben; CHEN, Yiling. Disparate interactions: An algorithm-in-the-loop analysis of fairness in risk assessments. In: Proceedings of the Conference on Fairness, Accountability, and Transparency, 2019.

Guide on Article 8 Of the European Convention On Human Rights (2020) [pdf] Council of Europe/European Court of Human Rights. Available at: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> [Accessed 25 September 2020].

Guidelines 3/2019 On Processing of Personal Data Through Video Devices. [pdf] European Data Protection Board, 2019. Available at: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf> [Accessed 25 September 2020].

HOFFMAN, David, 2014. Europe's New Right to Be Forgotten: Not New and Not Forgetting - Policy@Intel. [online] Policy@Intel. Available at: <https://blogs.intel.com/policy/2014/07/16/europes-new-right-forgotten-new-forgetting/#gs.fis0to> [Accessed 25 September 2020].

KOFMAN, Ava, 2016. How A Facial Recognition Mismatch Can Ruin Your Life. [online] The Intercept. Available at: <https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/> [Accessed 25 September 2020].

Met.police.uk. n.d. Update on Facial Recognition. [online] Available at: <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/> [Accessed 25 September 2020].

Privacyinternational.org. n.d. Facial Recognition | Privacy International. [online] Available at: <https://privacyinternational.org/learn/facial-recognition> [Accessed 25 September 2020].

ROUSE, Margaret, 2019. What Is Black Box AI? - Definition from Whatis.Com. [online] WhatIs.com. Available at: <https://whatis.techtarget.com/definition/black-box-AI> [Accessed 25 September 2020].

Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence, 2020. [online] Available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273> [Accessed 25 September 2020].

TAIGMAN, Yaniv, et al. Deepface: Closing the gap to human-level performance in face verification. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2014.

Tillsyn Enligt EU:S Dataskyddsförordning 2016/679 – Ansiktsigenkänning För Närvarokontroll Av Elever. [pdf] Datainspektionen. 2020. Available at: <https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf> [Accessed 25 September 2020].

Us.norton.com. 2020. How Does Facial Recognition Work? [online] Available at: <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> [Accessed 25 September 2020].

VON DER LEYEN, Ursula, 2019. A Union That Strives for More - My Agenda for Europe. [pdf] Brussels. Available at: <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf> [Accessed 25 September 2020].

WHITE PAPER on Artificial Intelligence - A European Approach to Excellence and Trust, 2020. [pdf] Brussels: European Commission. Available at: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [Accessed 25 September 2020].

Yourdictionary.com. n.d. Chilling-Effect Dictionary Definition | Chilling-Effect Defined. [online] Available at: <https://www.yourdictionary.com/chilling-effect#law> [Accessed 25 September 2020].