ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo 37

Settore Concorsuale: 12/G1 - DIRITTO PENALE

Settore Scientifico Disciplinare: IUS/17 - DIRITTO PENALE

RISKS OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS IN PUBLIC PLACES FOR LAW ENFORCEMENT PURPOSES UNDER THE AI ACT REGULATION

Presentata da: Cristina Domingo Jaramillo

Coordinatore Dottorato

Monica Palmirani

Supervisore

Monica Palmirani

Esame finale anno 2025

To my family.
My father Manuel and my mother Marisol.
And my sister Marisol.
Thank you for being patient and understanding even on my grey days.

ABSTRACT

The use of biometric technologies is becoming increasingly prevalent, serving purposes ranging from simple identity verification for granting or denying access to electronic devices or physical spaces, to more critical applications in the field of security. In the latter context, law enforcement institutions and officials are employing biometrics to prevent and control criminal activity. This technology proves highly effective in achieving such goals, as it enables the rapid identification of individuals, even within large crowds, based on specific physical or behavioural characteristics.

The anticipated security benefits of biometric systems are significant and, until now, largely unprecedented. However, their implementation also raises profound concerns regarding the fundamental rights and freedoms of citizens. This generates a contentious debate over whether the priority should lie with enhancing security—an imperative increasingly pressing due to the threats posed by terrorism and serious crime—or preserving individual liberties. The debate is particularly intense in relation to facial recognition-based biometrics, a technology widely adopted in numerous countries, where it has been shown to impose substantial restrictions on personal freedoms. Consequently, calls for its prohibition have emerged in certain contexts.

Despite these concerns, the European Union has opted to regulate biometric technologies under the Artificial Intelligence Act (AIA). While the AIA initially seeks to prohibit real-time biometric systems due to their intolerable risks to fundamental rights, it includes several exceptions that may allow their use in specific scenarios. This creates the potential for the technology's application to expand beyond its original intent. Conversely, systems operating in a delayed mode are classified merely as high-risk, subject to less stringent requirements and safeguards, thereby heightening concerns that improper use could lead to mass surveillance.

In light of the controversies surrounding this regulatory framework, this study examines the provisions of the AIA concerning remote biometric identification systems, with a particular focus on facial recognition technologies. It further analyses the implications of these systems for citizens' rights and freedoms, juxtaposed against the expected security benefits, to assess whether their use by states is justified or if their prohibition is warranted.

INDEX

ABBREVIATIONS 1

INTRODUCTION 3

CHAPTER I

INTRODUCTORY ISSUES

I. APPROACH TO THE WORKING TERMS 15

1. Artificial Intelligence systems 15

1.1. Some preliminary aspects about the development of these mechanisms 15

1.2. Different perspectives on the definition of AI 17

1.3. Types of artificial intelligence systems 19

1.4. Modalities of Artificial Intelligence 23

2. Biometrics and biometric data 25

2.1. What is biometrics 25

2.2. Biometric data 27

2.3. Differentiating biometric identification from emotion detection and biometric categorization 29

2.4. Functions of biometric systems: identification and identity verification 31

3. Remote biometric identification systems especially facial recognition 33

3.1. Ways in which FRs operate 34

3.2. Definition of facial recognition systems 35

II. NEW CHALLENGES POSSED BY CRIME THAT MERIT THE ADOPTION OF NEW CONTROL MESURES 37

III. INITIAL INTRODUCTION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN CRIMINAL MATTERS 42

1. AI and its relation with criminal commission 43

2. AI as a tool for preventing and fighting crime 48

CHAPTER II

APPROACH TO THE WAY OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS OPERATE AND THEIR REGULATION IN THE AI ACT

I. HOW BIOMETRIC IDENTIFICATION SYSTEMS WORK 57

1. Previous aspects 57
2. Digitalization of data 58
3. Phases of the data collection and storage process 58
4. Distinction between verification and identification functions 61
II.HISTORY OF THE USE OF BIOMETRICS IN THE FIELD OF DELINQUENCY 63
1. Advances in general biometrics 63
2. Approach to the evolution and operation of facial recognition systems 70
III.REGULATION OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS IN THE AI ACT 82
1. Previous approaches to the AIA 82
2. Classification of RBIS with law enforcement purposes in public places 85
2.1. Remote biometric identification systems on real time 88
2.1.1.Specification of the elements that constitute the prohibition of RBIS in real time in public access spaces with law enforcement purposes 89
A.Publicly accessible space 89
B.Law enforcement authority 90
2.1.2. Exceptions to the ban of use of real-time mechanisms stablished in the art. 5.1.h) AIA 91
2.2. Delayed remote biometric identification systems 96
2.2.1. Delayed RBIS term 97
2.2.2. Conditions of use according to the AIA and data protection regulations 98
2.2.3. Case study: Implementation of a delayed face recognition system by the national police in Spain 102
3. Common aspects of high-risk AIs 104

CHAPTER III

IMPACT OF FACIAL RECOGNITION SYSTEMS ON CITIZEN RIGHTS AND FREEDOMS

I. INITIAL ISSUES RELATED TO DATA SURVEILLANCE 111
II.FACIAL IMAGES AS BIOMETRIC DATA 113
1. The face as a particularly sensitive private data 113
2. Distinction of the face with other biometric parameters: intrusiveness issues 116

3. Availability of the face in public places 119
III.IMPACT ON FUNDAMENTAL RIGHTS AND FREEDOMS 121
1. Human rights in their private dimension 123
1.1. Human dignity..... 123
1.2. Privacy 126
1.2.1.Approach to the concept of privacy 126
1.2.2.How privacy is affected by FRs..... 129
1.2.3.Privacy in public space and the interference with the use of FRs 130
1.2.4.The right to privacy as a limit to state power 133
1.3. Data protection..... 138
1.3.1.Distinction between the privacy and data protection rights..... 139
1.3.2. .. Circumstances that promote the necessary protection of personal data..... 141
1.3.3.Biometric face parameters in public places with law enforcement purposes and the data protection right 143
1.3.4.Sources from which face information is extracted: what happens with images published on social networks?..... 146
1.3.5.Combination of data protection and artificial intelligence regulatory provisions in the field of RBIS 151
1.3.5.1.Regulation of bioemtric data processing 153
1.3.5.2.Consent, Strict necessity and essential public interest 154
1.3.6.Requirements on data processing and their storage in databases 158
1.3.6.1.Lawful, fair and transparent..... 158
1.3.6.2.Specific, explicit and legitimate purpose..... 162
1.3.6.3.Data minimisation, accuracy, storage limitation, data security and accountability 165
1.4.Personal identity 169
1.5.Self-image..... 173
1.6.Freedom of movement..... 175
2. Individual freedoms in their social dimension: expression, association, reunion, demonstration and strike..... 179
3. Prohibition of discrimination 183
3.1.Algorithmic discrimination..... 186
3.2.Direct and indirect algorithmic discrimination..... 190

3.3.Errors and biases 192
3.4.Black boxex 195
4. Presumption of innocence and other rights in the field of criminal law 198
5. New rights on the digital field 201
5.1.Human intervention in aumatic decision-making processes 201
5.2.Right to be forgotten 202
5.3.Access to information: right to know how the algorithm works 203
IV. LIMITS TO FUNDAMENTAL RIGHTS: PROPORTIONALITY AND STRICT NECESSITY CRITERIA 204
1. Provided for in a specific law 205
2. Proportionality test 212
3. Strict necessity in a democratic society 218
4. Specific cases in which facial recognition system can be used according to the article 5.h) AIA 220
V. OTHER PROBLEMS DERIVED FROM THE USE OF FACE DATA IN BIOMETRIC IDENTIFICATION SYSTEMS 225
1. Function creep 225
2. Mass surveillance state 228

CHAPTER IV

POLICE ROLE IN MAINTAINING SECURITY AND THE RISK OF MASS SURVEILLANCE ARISING FROM THE USE OF FACIAL RECOGNITION SYSTEMS

I. APPROACH TO THE TERM SECURITY 237
II. POLICE FUNCTION OF MAINTAINING SECURITY IN A DEMOCRATIC STATE 244
III. DEBATE BETWEEN FREEDOM AND SECURITY 250
1. General aspects 250
2. Need to find a right balance: special reference to the *Osman Test* and police knowledge of the existence of a security threat 252
3. Maintaining security as argument for adopting generalized surveillance measures that restrict rights 256
IV. SECURITY AN SAFETY BENEFITS PROVIDED BY FACIAL RECOGNITION SYSTEMS 260

V. NEW TRENDS IN SOCIAL CONTROL AND SECURITY MAINTENANCE THROUGH DIGITAL SYSTEMS. ESPECIALLY FACIAL RECOGNITION 264

1. The "Banality of goods" used to guarantee security 266

2. Digital panopticon 268

2.1.General approach to the panoptic theory 268

2.2.The role of new technologies in the spread of the digital panopticon 269

2.2.1. .....Change of direction: from a disciplinary society to a control society 270

2.2.2.The panoptic in the age of algorithms: What is happening with facial recognition systems? 273

CONCLUSIONS 281

BIBLIOGRAPHICAL APPENDIX

BIBLIOGRAPHY 301

WEBGRAPHY 329

LEGISLATION 335

International 335

Europe 335

European Union 335

Spain 337

Italy 337

France 337

RECCOMENDATIONS AND OTHER TEXTS 338

JURISPRUDENTIAL APPENDIX 340

Court of Justice of the European Union 340

European Court of Human Rights 340

Spain 342

Italy 342

United Kingdom 342

Germany 343

France 343

ANNEX I 345

ABBREVIATIONS

A29 WP:	Article 29 Data Protection Working Party
AI:	Artificial Intelligence
AIA:	Artificial Intelligence Act
AIs:	Artificial Intelligence system
API:	Automated Personal Identification
DL:	Deep Learning
CAHAI:	Ad hoc Committee on Artificial Intelligence
CCTV:	Closed-Circuit Television
CNN:	Convolutional Neural Networks
Coord./s.:	Coordinator/s
DNN:	Deep Neural Networks
ECHR:	European Court of Human Rights
Ed./s.:	Editor/s
EDPB:	European Data Protection Board
EDPS:	European Data Protection Supervisor
FR:	Facial Recognition
FRA:	European Union Agency for Fundamental Rights
FRs:	Facial Recognition system
GDPR:	General Data Protection Regulatoin
IAFIS:	Integrated Automated Fingerprint Identification System
ICT:	Information and Communication Technology
IMY:	Swedish Authority for Privacy Protection
IoT:	Internet of Things
LEA:	Law enfocement authorities
LED:	Law Enforcement Directive
LFW:	Labeled Faces in the Wild dataset
ML:	Machine Learning

NATO:	North Atlantic Treaty Organization
NS:	National Security
NSS:	National Security Strategy
OECD:	Organization for Economic Co-operation and Development
RBIS:	Remote Biometric Identification System
SCC:	Spanish Constitutional Court
SDPA:	Spanish Data Protection Agency
STA:	Security Threats Assessment
UNESCO:	United Nations Educational, Scientific and Cultural Organization
Venice Commission:	European Commission for Democracy Through Law

INTRODUCTION

New information and communication technologies (hereafter ICTS) have revolutionised society. What was once a novelty has now become ordinary. In this sense, practically all the activities we carry out on a daily basis are conditioned by technology, even controlled by it[1]. Citizens live in a state of hyperconnection to all kinds of electronic devices, which offer innumerable advantages but also introduce new risks, especially in terms of affecting the fundamental rights and freedoms of the population, both at the individual and social level. This is due, among other things, to the fact that most of them operate with personal data.

One of the emerging technologies that is having the greatest impact and expansion is Artificial Intelligence (AI). Its use is becoming more and more widespread and reaches very diverse activities given that, for example, it can be found in word processors as a spell-checking tool, translators, even sophisticated image or video creation programmes, among many other functions, such as choosing the music we listen to and the films we watch. It is also capable of creating profiles and, in the business world, it influences decision-making in finding and keeping a job; in the medical field, it chooses and proposes treatments, etc. As can be seen, in the world of smart devices (also known as the Internet of Things, IoT), algorithms are a constant and are present in practically every social environment. The mathematical processes through which such mechanisms operate are fed by the huge amount of data that is constantly being produced today, which can even be generated by the users of electronic devices themselves. Such is their importance and value that they have come to be considered the oil of the XXI century.

Law and, of course, criminal law, has not remained outside of this evolution and, nowadays, automated systems have also reached this environment, being present in practically all stages of the process. Thus, they alert the police to the possible commission of a crime, enabling better management of resources, they decide whether it is necessary to initiate judicial proceedings or to order pre-trial detention, they propose sanctions, etc.[2]

In the context of our research, the police use of remote biometric identification systems (hereafter RBIS), specifically facial recognition (FR), allows the recognition of –among others– victims and missing persons, as well as possible suspects of having committed a serious crime or terrorists in publicly accessible places, also known as uncontrolled spaces. They are known as such because the biometric device is located in

[1] In this sense, the impact of these new developments also affects the law, since it is responsible for responding to the new questions and requirements that arise. In this opinion, ALBA CATOIRA, A. 'La garantía de los derechos como respuesta frente a los retos tecnológicos', in Balaguer Callejón, F. & Cotino Hueso, L. (Dirs.), *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, pp. 58-59.

[2] BALAGUER CALLEJÓN, F. & COTINO HUESO, L. (Coords.), *Derecho público de la Inteligencia Artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios del Estado Autonómico, Zaragoza, 2023, p. 18.

an environment open to the public and can operate on any individual passing through it. In contrast, in controlled spaces, the systems can only be used with the consent of the individuals[3].

RBIS have not only become widespread in the field of law enforcement, for they are used as a tool that allows, among other things, to verify the identity of users of mobile devices or bank accounts, through the parameters of the face or fingerprints, allowing – or, as the case may be, denying– access to them. Furthermore, some authors argue that biometric systems are currently necessary for the verification and identification of individuals, due to the increase of human factors in new generation technologies[4]. In addition, these recognition and identification techniques based on physical or behavioural characteristics have proven to be useful in both the public and private sectors[5]. This is based on the understanding that the parameters with which they work are unique to each person and normally invariable, which will allow identification over time, and are more effective than passwords or other alphanumeric personal identifiers that are susceptible to being forgotten or stolen.

In view of the usefulness of biometric technologies, they have rapidly become a central element of contemporary Governments. This trend follows an evolutionary trajectory of identity systems, from the introduction of surnames, citizen ID numbers, the integration of biometric data in passports and the use of DNA in police investigations, to algorithms that allow automated association of this data with specific individuals, all of which have made people distinguishable to both corporate and state actors. The novelty of the introduction of automated recognition systems in the public domain by law enforcement authorities (LEAs) is that they allow the categorisation, attribution and establishment of simple identities using digital representations of body parts (such as face, iris, ear shape, etc.) or even behaviour "in the wild" and in "real-time" or in a very short time frame.

Not only systems that act immediately are used, since they can also operate with a delay or over a longer period, and there are two types of RBIS depending on the time they take to carry out identifications. This distinction is set out in the Artificial Intelligence Act (from now on, AIA)[6] which, as we will have the opportunity to explain throughout this research, also establishes different regulations for both types according to

[3] EDPB. *Guidelines 3/2019 on processing of personal data through video devices*, version 2.0, 29 January 2020, p. 21.

[4] TASKIRAN, M. et al. "Face recognition: Past, present and future (a review)", *Digital Signal Processing*, vol. 106, 2020, p. 1.

[5] REDING, V. "Foreword. Privacy Implications of Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. V; JANSEN, F. et al. "Biometric identity system in law enforcement and the politics of (voice) recognition: The case of SiiP", *Big Data & Society*, vol. 8, nº. 2, 2021, p. 1.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulation (EC) No 300/2008, (EU) No 16/2013, (EU) No 168/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

the different level of impact they have on citizens' rights and freedoms. The former, i.e. those deployed in real time, are initially prohibited because they are considered to be an intolerable interference in the rights and freedoms of the population, while those that act in delayed mode, although not prohibited, are considered high-risk and, for this reason, their use must be governed by the common requirements for this type of devices established in the Regulation. The latter also regulates other biometric recognition mechanisms used in law enforcement to prevent crime, such as emotion detection. However, as interesting as this technique is in terms of its implications and the controversies it generates, it will not be analysed at this point, since, given its complexity, it would require a separate, in-depth study. On the other hand, we also do not focus on FRs deployed in the private sphere or those that, although used in the public sphere, have purposes other than the fulfilment of the law.

Therefore, our study focuses specifically on the RBIS used in the public sphere by LEAs for law enforcement purposes, on their regulation through the AIA and the risks that arise –or may arise– in relation to the rights and freedoms of the population as a result of their implementation and other associated problems. This is because we are faced with the paradox that, on the one hand, there is a desire to act as a stronghold in defence of rights and, on the other, there is a temptation to resort to promises of recognition and identification using AIs to control threats to public order, which can lead to confusing between protection and repression or terrorism with activism[7].

As the parameters used for identification through biometrics are many and varied, we will focus specifically on the face, because of the existing debate about the use of FRs between their advocates and detractors. Moreover, it has been one of the most controversial issues of the AIA, one of the most modified since the first proposal for the Regulation was published in 2021, which has led to a delay in its entry into force until 13 June 2024. Despite the fact that different international institutions and organisations requested its prohibition or a moratorium on its deployment until the state of the art is more advanced, finally, due to pressure from the Member States of the European Union (EU), its regulation was accepted in the terms that will be analyzed throughout this study.

In this regard, it is worth noting that the AIA, in general, is very relevant because it is the first regulatory text in which public institutions address the issues of AI or, more precisely, AI systems (AIs). It is thus a comprehensive, cross-sectoral and supranational attempt to regulate AIs and algorithmic products from a risk-based approach[8]. Thus, it classifies the instruments at different levels, distinguishing AI technologies according to

[7] RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 380-381.

[8] KIND, C. "Containing the canary in the AI coalmine-the EU's efforts to regulate biometrics. Exploring the gaps and risks relating to biometrics in the EU's draft AI regulation", *Ada Lovelace Institute*. Recurso electrónico obtenido a través de la Web: https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/, [retrieved on 8 May 2024].

the danger they pose to fundamental rights. Among them, as we pointed out above, are those that form our object of study, that is, the RBIS, including the FRs.

The regulation of some controversial technologies such as the one constitutes our research, as KIND states, "have acted as a canary in the AI coalmine, provoking individual alarm and societal debate about the role of AI in our societies"[9]. One of the biometric parameters which use is becoming increasingly widespread in the field of crime prevention and control, given its effectiveness, is the FRs[10]. This mechanism has improved and accelerated the process of identifying people by the police, who can respond in real time in relation to an individual who is committing or suspected of committing a crime. They can stop and arrest him or take preventive action, thereby increasing the preparedness of police officers in a given area for the presence of suspects. It can not only identify a subject's face in a large crowd, but also detect emotions and affections.

In that sense, these systems can be used to detect strange behaviour that could lead to arrest and initiate proceedings against someone[11]. Such is the extent of their expansion that they have come to be considered the "holy grail" in the field of state surveillance[12] and, in fact, are the most important technological advance on the horizon of Closed-Circuit Television (CCTV). As SKOGAN rightly points out, FRs promise to "put name to faces on a massive scale with enough accuracy to guide further investigations or to intervene in situations"[13]. As we have said, these technologies have a great impact on our daily lives and can even lead individuals to decide not to exercise their rights in the public sphere for fear of being victims of the sometimes excessive surveillance.

Despite the above, we have to be aware that their use is already unavoidable[14], given that they are included in the AIA. For this reason, the focus of our study has been on analysing the potential harms that may arise from their deployment and the requirements and safeguards that the mechanisms should observe to ensure that their use is as limited and proportional as possible to the intended purpose. The potential of these technologies is still unknown, as is the way in which they impact fundamental rights and freedoms and, therefore, our daily lives.

---

[9] *Ibd.*

[10] As early as 2001, WOODWARD predicted that FR technology would expand as it proved increasingly effective. WOODWARD, J.D. *Super Bowl surveillance. Facing up to biometrics*, RAND Arroyo Center, 2001, p. 5. Such an extension is already evident and its use is becoming more and more common in different fields and activities.

[11] NOVOKMET, A. et al. "Facial recognition technology in EU criminal justice-human rights implications and challenges", *Digitalization and Green Transformation of the EU,* vol. 7, 2023, p. 550.

[12] INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance: The politics of facial recognition systems", *Surveillance & Society*, vol. 2, nº. 2/3, 2004, p. 178.

[13] SKOGAN, W.G. "The future of CCTV", *Criminology and Public Policy*, vol. 18, nº. 1, 2019, p. 164.

[14] MURRAY, D. "Facial recognition and the end of human rights as we know them?", *Netherlands Quarterly of Human Rights*, vol. 42, nº. 2, 2024, p. 146.

For all of the above reasons, a question immediately arises, which we will try to answer throughout this research: Is the use of FRs appropriate and in line with citizens' rights and freedoms in the EU according to the regulation established in the AIA? In this sense, the hypothesis is that the regulation of FRs in the AIA may not be accurate in relation to the risks they entail when the security benefits are still unknown.

In order to provide an adequate response, we try to achieve some goals from the following objectives:

General Objective: To understand the risks posed by RBIS, especially FRs in terms of compliance with the law in public places as a result of the provisions of the AIA and the benefits they entail in terms of security.

To reach this goal, we set out to meet a number of specific objectives:

- Specific Objective 1. To study the AIA and related regulations, such as those regarding to the protection of personal data.
- Specific Objective 2. To understand how they regulate the mechanisms under study.
- Specific Objective 3. To establish the distinction between the types of FRs in the public sphere for law enforcement purposes.
- Specific Objective 4. To identify the risks that FRs pose for citizens, especially in terms of fundamental rights and freedoms and other associated problems.
- Specific Objective 5. To determine whether it is possible to limit the exercise of the rights and freedoms of the population and the requirements for doing so.
- Specific Objective 6. To approach the benefits of FRs in security.
- Specific Objective 7. To analyse whether the widespread use of FRs leads to a situation of mass surveillance.

With the aim to achieve the proposed objectives and to gain a comprehensive understanding of all the aspects that revolve around the FRs, the methodology used to develop the study must also be comprehensive. Firstly, a systematic review of documentary sources was carried out, selecting the most relevant and current bibliography. To this end, we used the databases available at the Library of the European Court of Human Rights (ECHR), where a two-month research stay was carried out, as well as those of the Universities of Bologna and Granada, both in physical and digital format. In addition, specialised databases such as Scopus, ProQuest, Google Scholar and Dialnet were used.

The regulations have been extracted from the official institutions, such as the *Official Journal of the European Union*, the *Council of Europe* and the *Spanish Official State Gazette*. The main regulatory sources used are the AIA, the specific one on personal data protection: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) and, specifically for our field of study, for deploying FRs in the field of law enforcement, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive, LED); and that related to human rights in general. In this case, the Charter of Fundamental Rights of the European Union (2012/C 326/02) and the European Convention on Human Rights of the Council of Europe.

In addition to the above, existing jurisprudence on human rights and policing, both national and international, has been used, especially that issued by the ECHR and the Court of Justice of the European Union (CJEU). To complement this, we have also resorted to specific jurisprudence on FRs, which is not very abundant at the moment, given that there are only two court Judgements, one in England and another by the ECHR against Russia. The latter Judgement is very interesting and highly relevant, given that it is the first in which an international institution has taken a position on the issue. We also added an interview in semi-structured format with the Head of the Identification Unit of the Scientific Police of the city of Granada (Spain)[15]. The latter allows us to learn about the way in which FRs are being implemented in the aforementioned country, where they began to be used at the end of 2023 in the delayed mode.

The thesis is structured as follows. Firstly, it is composed of four main chapters in which all the issues under study are analyzed, an introduction and conclusions, an index of abbreviations and a bibliographic appendix. The latter has been divided into different sections, in which each and every one of the references used are listed in alphabetical order and date of publication: monographs, collective works, book chapters, scientific and journalistic articles, as well as regulations and other texts from national and international organisations and institutions on the subject of study. This is followed by a jurisprudential appendix that systematically collects the judicial pronouncements taken into account for our research, classified by the sentencing body and date of resolution. The thesis closes with an annex that includes the structure followed to carry out the aforementioned interview with the Head of the Identification Unit of the Scientific Police of the National Police Corps of the city of Granada and a final note.

Chapter I, called "introductory issues", addresses various general issues that will lay the foundations for the subsequent development of the other parts of the Thesis. Thus, it begins with the specification of some key concepts, such as AI and AIs, biometrics and biometric data, reaching RBIS and the definition of FRs. Next, the new risks posed by

[15] For more information on the structure and issues raised, see Annex I.

technological advances in the commission of crimes are raised and how, on the other hand, they are a useful tool in their control and prevention.

Chapter II, entitled "Approach to the way of remote biometric identification systems operate and their regulation in the AI Act", is divided into several parts. On the one hand, the question of the way in which these systems operate is addressed, from the previous phase of data digitization, through the different steps of their collection and processing until reaching the moment in which they carry out the identification. This is essential to understand how they can impact the lives of citizens and the benefits in terms of security. Furthermore, a distinction is made between the identification and verification functions because both are considered differently in the AIA, while the latter is not even included in it. The historical evolution of biometrics in the police field in general is then presented, and then, the FRs. This leads to the regulation of the RBIS in the AIA, highlighting the classification made on those that act in real time and in deferred time based on the different level of risk that each of them entails in rights and freedoms and the distinction in terms of requirements and elements that must be observed depending on whether it is one or another typology. As the FRs used in Spain act in deferred time, the results of the interview have been inserted at this point as a case study to be considered as an example of the way in which the LEAs are resorting to this technology in the country.

Once the above has been done, Chapter III focuses on the impact of the RBIS on the rights and freedoms of citizens. As an introduction, some issues related to surveillance based on data and algorithms are briefly addressed, as well as the reasons why the image of the face must be considered biometric data and, due to its characteristics, especially sensitive and visible to the eyes of others and susceptible to being captured by FRs. Having established the previous issues, the impact of the fundamental rights and freedoms of these instruments is addressed with all the intervening elements, not only individual but also collective, from a holistic and comprehensive approach, given that the influence on one of them affects the others. They have been classified into different groups as follows: firstly, individual rights are addressed in the private dimension, including human dignity, privacy, protection of personal data, personal identity, self-image and freedom of movement; individual freedoms in the social dimension, among which are the freedoms of expression, association, assembly and demonstration. Due to its importance, a separate section has been devoted to the prohibition of discrimination with the different elements that may favour it through the use of automated identification mechanisms, including errors and biases and black boxes. Next, procedural rights are addressed, more specifically the presumption of innocence, since it is seriously threatened by these systems, especially when the results they produce are not correct; and, finally, some of the new rights that are emerging in the digital landscape related to such mechanisms are set out, such as human intervention, the right to be forgotten and access to information. The fourth section of this third chapter is devoted to the requirements by which the aforementioned rights and freedoms may be limited, with special emphasis on the criteria

of proportionality and strict necessity, while the others were set out when the analysis of the right to the protection of personal data was carried out according to the regulation done by the LED in conjunction with the provisions of the AIA. This is because it is the right most affected, due to the fact that identification is based on the facial data of individuals, for which there is specific regulation that limits and specifies the elements to guarantee an adequate use of the mechanisms. As a culmination of this Chapter, some resulting problems are studied, such as the function creep or extension of the instruments to purposes other than those initially established and the possible mass surveillance of society.

Finally, Chapter IV, about the "police role in maintaining security and the risk of mass surveillance arising from the use of facial recognition systems", begins with the concept of security and its different meanings, establishing citizen security as that which is intended to be protected and guaranteed with the use of FRs in the area of compliance with the Law. Once the above has been specified, the essential function of the social and democratic State in maintaining security is studied, materialized through the police and the need for its actions not to exceed certain limits. This leads to the debate between security and freedom of exercise of rights, concluding the need to find an adequate balance between the two and rejecting that the former is erected as an argument to adopt systems that favour the implementation of restrictive measures of the latter. The fourth part of this Chapter is aimed at presenting the benefits observed by FRs in terms of safety and security, identifying victims of crimes and missing persons on the one hand, and in prevention and control of crime on the other, through the detection of criminals not only when they have committed the crime but also when there are threats of perpetrating it. Finally, as FRs are a digital mechanism intended to guarantee social control, the different trends in this environment introduced by virtual systems are presented, as well as how citizens themselves are able to exercise control over others through electronic devices. Not only that, but the fact that RBIS, video surveillance systems and other CCTV are common instruments means that society is not fully aware of the risks it faces, often legitimising their use without taking into account the dangers they entail.

For all the issues mentioned above, our research is novel and relevant for several reasons. Firstly, because it covers the analysis of the regulation of the RBIS by the AIA, whose entry into force which, at the time of writing these lines, is very recent, which is why, to date, there are not many studies on the subject. Secondly, in view of the risks and dangers to citizens' rights and freedoms that come with using such instruments, especially FRs in the public sphere for the purposes of compliance with the Law, as a mechanism that aims to guarantee security through the identification of suspected criminals and terrorists, both once the crime has been committed and at a previous time, in order to prevent threats of its perpetration. A third reason is found in the approach used to analyse the civil rights and guarantees at risk of injury, given that most existing studies, with a limited perspective, focus on one of them (specifically on the protection of personal data right or privacy), while in the present research a comprehensive approach is made to all

those affected, in a relation of interdependence, since the limitation of one impacts on the others and causes other associated problems. The fourth is based on the fact of comparing the above with the expected benefits in terms of security, because the supposed increase in the latter is one of the arguments used by the defenders of the technique, without considering –or underestimating– the impact on those.

As can be seen from what is immediately stated, the study introduced here does not focus only on the FRs from a single perspective, that is, from the normative point of view, addressing the ethical and legal implications[16]; nor exclusively on the expected risks and benefits. On the contrary, a complete and comprehensive study is produced in which all the aspects mentioned are combined and this represents a great novelty and advance in the study of FRs.

[16] Some studies focus on this, see for example, ORIT, K. *In the face of ethics police use of live facial recognition technology*. Thesis submitted for the degree of Doctor of Philosophy (PhD) in Law, London, May 2024.

CHAPTER I
INTRODUCTORY ISSUES

I. APPROACH TO THE WORKING TERMS

1. Artificial Intelligence systems

1.1.Some preliminary aspects about the development of these mechanisms

The first task to be addressed in this first chapter is the definition of AI and AIs, since the biometric identification mechanisms that constitute our object of study are often a specific type of AI, acting mainly through *Deep Learning* systems (from now on, DL). There is no consensus on the establishment of a concept of AI, and there are multiple definitions that vary according to the discipline that tries to address it and the objectives that are intended to be achieved with it[17]. Likewise, independent organizations and national and international legislators –with greater or lesser success– have tried to define the term.

The situation just described is not exclusive to AI, the conceptualization of natural intelligence is problematic since there is no single, shared term for it. However, it is generally agreed that intelligence refers to the capacity to perform different actions, among which are adaptation to the environment (especially to new situations), learning through experience, perception, intuition, etc.[18] AI is inspired by intelligence but its goal is not only to study it but also to build it, i.e., to give life to intelligent instruments[19]. On the other hand, it is important to emphasize that AI is not the same as human intelligence, since the autonomy of intelligent mechanisms is deprived of mental perception and the moral values involved in certain choices[20]. Following FINOCCHIARO, intelligence is attributed to human beings or to animals. So using this term linked to machines induces to create a narrative in anthropomorphic terms, since if AIs are intelligent, then there is a being (either human or animal) to whom intelligence is attributed[21] , when this is not the case. For that reason, the author considers that it would be more appropriate to refer to it as *machine learning*, i.e., machine learning system based on the use of data, as will be

[17] VALLS PRIETO, J. *Inteligencia artificial, Derechos humanos y bienes jurídicos,* Aranzadi, Navarra, 2021, p. 18. The author exposes four major definitions of AI that can overlap, classified according to the capacity of the mechanisms to: process thought and reasoning, behaviour, human performance and ideal performance. Thus, he goes on to assert, any machine that behaves like a human can be considered an AI.

FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?*, Il Mulino, Bologna, 2023, p. 21, also echoes this question and assures that it is a difficult operation and many definitions have appeared, especially in recent years, when the subject has received widespread attention.

[18] SARTOR, G. *L'intelligenza Artificiale e il Diritto*, Giappichelli, Torino, 2022, p. 1.

[19] *Ibd.*, pp. 2-5. The purpose of application of AI, i.e., whether for the purpose of simulating man or to cope with certain tasks efficiently, will determine the distinction between the work of reproducing human thought and the work of developing rational cognitive processes.

[20] D'ALOIA, A. "Ripensare il Diritto nel tempo dell'Intelligenza Artificiale", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, p. 87.

[21] FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?*..., cit., p. 23.

discussed below[22]. Leaving aside questions relating to the link between AI and human intelligence, since it is far beyond the scope of our object to study, we will approach the definition of AI and its evolution.

In this regard, it should be noted that, although it may seem a new issue in view of the rapid expansion it is currently undergoing, AI emerged some decades ago. In 1950 Alan Turing started to speak about it in his article *Computing machinery and intelligence*, in which he argued that an intelligent machine seemed more human if it was capable of thinking like a person, rather than just resembling one. This approach is the one that has remained to this day[23]. However, it was not until the summer of 1956 that such an expression was first used by John McCarthy at a conference on AI held at Dartmouth. This technology has had some ups and downs, but is currently experiencing a "golden age"[24] and its use –as previously stated– is growing due to the great development it has undergone in recent years, motivated by the confluence of different factors: massive data production by citizens using cell phones, a strong data processing capacity, as well as a good development of computer engineers[25].

The progress of AI has been of such magnitude and in such varied fields that its use has been extended to a multitude of contexts and uses, while at the same time being opaque. This has led to a proliferation of concepts, making it difficult to define what AI is[26]. It is therefore very difficult to establish a definition that is both precise and exhaustive, since we are faced with a wide range of methods and techniques applied to a broad set of scientific, technological and industrial objectives. This is even more difficult in the case of the legal interpretation of the term, which, according to SARTOR, can only be teleological in order to be able to cover as many of the systems that present the risks and opportunities of intelligent applications as possible[27].

---

[22] *Idem*. On p. 29 of the same work, he argues that if an anthropomorphic discourse is adopted, there is a risk that the discourse will be reconstructed in terms of subjectivity.

[23] GUO, T. "Alan Turing. Artificial intelligence as human self-knowledge," *Anthropology Today*, vol. 31, no. 6, 2015, p. 3. See also, at greater length, COPELAND, J. *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life: Plus The Secrets of Enigma*, Oxford University Press, New York, 2004, pp. 442 and the next.

[24] On the history of AI and the different periods through which it has passed, SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit., pp. 23-33.

[25] VALLS PRIETO, J. "Sobre la responsabilidad penal por la utilización de sistemas inteligentes", *Revista Electrónica de Ciencia Penal y Criminología*, vol. 24, nº. 27, 2022, p. 3.

[26] HAYWARD/MAAS criticize this lack of a precise definition, as they consider that it causes confusion. HAYWARD, K.J. & MAAS, M.M. "Artificial intelligence and crime: A primer for criminologists", *Crime Media Culture*, vol. 17, nº. 1, 2021, pp. 210-211. Similarly, MUNARINI, M. "New perspectives on the mitigation of gender bias in AI by EU regulations", *Peace Human Rights Governance*, vol. 6, no. 2, 2022, p. 112. In the latter's view, the lack of a standard definition of what is considered AI and, consequently, an AI-driven technology, leads to imprecision in addressing progress and failures in this area.

However, for the Association for the Advancement of Artificial Intelligence, it is the absence of a precise and universally accepted term for AI that has helped it advance more rapidly. ASSOCIATION FOR THE ADVANCEMENT OF ARTIFICIAL INTELLIGENCE. *Artificial Intelligence and Life in 2030*, 2016. Electronic resource obtained from the World Wide Web: https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, [retrieved on 2 November 2023], p. 3.

[27] SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit., p. 9.

If, as we pointed out above, there is not even a shared concept of intelligence and it is not possible to distinguish precisely what is intelligent from what is not, this complicates the task of differentiating between computer systems that can be understood as intelligent and those that cannot. In the following pages, some of the many definitions that have been established about this phenomenon will be presented from a critical perspective. In this regard, it should be noted that not all of them will be reproduced, since this task is far beyond the scope of our study. Therefore, we will only consider those that, in our opinion, are more in line with the legal perspective of the term.

1.2.Different perspectives on the definition of AI

From a general approach, AI can be defined as the ability of machines to learn and perform cognitive tasks that were previously limited to humans, being able to imitate (or, rather, simulate[28]) or even surpass human cognitive abilities[29]. Along similar lines, the Council of Europe understands AI as the set of sciences, theories and techniques aimed at improving the ability of machines to do things that require intelligence. Thus, a system of this type is capable of making recommendations, predictions or decisions to meet specific objectives[30]. More specifically, UNESCO, although aware that a single definition is not possible, given that it may evolve over time due to technological development, in the *Recommendation on the ethics of artificial intelligence* adopted in Paris on 23 November 2021, understands it as those "systems which have the capacity to process data and information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control".

The above definition does not include the human component that was considered essential for training and defining the machine's objectives, which is provided for in the definition offered by the OECD in the *Recommendation of the Council on Artificial Intelligence*, which refers to the definition of objectives by people[31]. Thus, each system

[28] In this sense, PÉREZ Y MADRID, emphasizes the ability of AIs to simulate operations, which is why he argues that it is not an intelligent system in the human sense, but a mere simulation. PÉREZ Y MADRID, A. *El reconocimiento facial es un superpoder. Cómo te afectará y por qué deberías conocerlo*, Dykinson, Madrid, 2021, p. 17.

[29] COMEST, *Preliminary Study on the Ethics of Artificial Intelligence*, Paris, 2019, p. 3. Similarly, BROADHURST, R. et al. *Artificial Intelligence and Crime. A Research Report for the Korean Institute of Criminology and the Australian National University Cybercrime Observatory*, 2018, p. 4. AIs copy human performances, learn by correlations and do not follow the deductive-casual reasoning characteristic of human intelligence, so the two types of intelligence are distinct. BASILE, F. "Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione", in Balbi, G. et al. (Dirs.), *Diritto penale e Intelligenza artificiale "nuovi scenari"*, G. Giappichelli Editore, Torino, 2022, pp. 3-4.

[30] COUNCIL OF EUROPE. *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*, 2019, p. 5.

[31] C/MIN(2024)16/FINAL. Likewise, the European Commission, in the Proposal for the AI Law of April 21, 2021, established in its art. 31 a definition of AIs (later modified in the final version, as will be explained below) in which it refers to these objectives. Thus, it understood as such, the software developed using one or more of the techniques and strategies of Annex I and that, for a given set of objectives defined by humans, can generate different output information: contents, predictions, recommendations or decisions that influence the environments with which it interacts.

will have a specific purpose that will speed up the decision-making process for the individuals who use it. Along these lines, there is also the definition offered in 2019 by the Artificial High-Level Expert Group on Artificial Intelligence in the *Ethics Guidelines for Trustworthy AI*, which establishes AI mechanisms as "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numerical model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions"[32].

Although we consider the latter to be very complete, for the purposes of our study and in view of the technological advances experienced in recent years, we must take into account that established by the AIA in art. 3.1, which defines an IA system as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"[33]. As can be seen, it combines the different elements of the above. As stated in recital 12, the definition offered is intended to be harmonized with the previous ones, in order to ensure legal certainty and facilitate international convergence and broad acceptance. Furthermore, it is intended to be flexible in order to favour adaptation to technological advances. However, it establishes some new features with respect to the previous term, since in this case it differentiates the former from the more traditional and simpler *software* or programming systems, and eliminates the reference to those based on rules defined only by natural persons to automatically execute operations. This is due to the inference capacity of the mechanisms that include automatic learning strategies that allow them to learn from the data how to achieve the objectives and perform the tasks. Thus, this capability transcends basic data processing, since it allows learning, reasoning or modelling. AIs are designed to function with different levels of autonomy, being able to have a certain degree of independence with respect to human action and have some capabilities to function without it.

All the above definitions refer to the mechanisms of AI, which are not the same as the scientific discipline of AI, which includes different approaches and techniques, such as *machine learning* (hereafter ML), which encompasses *deep learning* and

[32] The proposed definition includes many important functions of AIs. At this point it should be remembered that most of the instruments develop only one function (pattern recognition, translation, information filtering, information selection, etc.), while others combine several capabilities, such as autonomous vehicles that have to be able to identify the objects they encounter and to plan the path, as well as to steer themselves on the journey towards the goal. SARTOR, G. *L'intelligenza artificiale e il Diritto...*, cit., p. 8.

[33] Almost identically, the Council of Europe in art. 2 of the *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, nº. 225, 5 September 2024.

reinforcement learning; *machine reasoning* (planning, programming, robotics, knowledge representation and reasoning, search and optimization); and robotics (control, perception, sensors and actuators as well as the integration of all other techniques in cyber-physical systems)[34]. Thus, AI is configured as a discipline that materializes in systems endowed with a high computational-logical capacity with which large amounts of data and information can be elaborated and processed and decisions can be made in a multitude of fields[35] –in our case, criminal law and, more specifically, the maintenance of public safety[36]– with the aim of obtaining a specific result. Thus, such mechanisms have the possibility of performing automatic behaviours considered intelligent because they can execute them in a similar way to humans in a specific context in which they have to choose between different possibilities and offer useful solutions to people[37]. We also add that they can learn the means to achieve certain goals and strategies from the data.

1.3.Types of artificial intelligence systems

There are several types of AI mechanisms: those that base their learning on logical rules (*rule-based*) and those that based it on data (*data driven*, *neural networks*)[38]. The latter are trained to learn using a large amount of information. In this sense, it is necessary to bring up the term ML, specified in the *European Ethicar Charter on the use of Artificial Intelligence in judicial systems and their environment*, adopted by the European Commission for the Efficiency of Justice (CEPEJ), as the system that "makes it possible to construct a mathematical model from data, incorporating a large number of variables that are not known in advance. The parameters are configured gradually during the learning phase, which uses training data sets to find and classify links"[39]. This technique

[34] Artificial High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 36.

[35] In the public sphere, it has six hundred use cases. See all authors in work of COTINO HUESO, L. "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, nº. 63, 2023, pp. 2-3.

[36] AIs are very effective in the investigative activity of police forces in the field of crime investigation and prevention. In this sense, among others, PISTILLI, C. "L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine: tra prospettive di sviluppo ed esigenze di coordinamento", in Balbi, G. et al, (Dirs.), *Diritto penale e intelligenza artificiale "nuovi scenari"*, G. Giappichelli Editore, Torino, 2022, p. 149.

[37] VALLS PRIETO, J. *Inteligencia artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 19; and BROADHURST, R. et al. *Artificial Intelligence and Crime...*, cit., p. 4.

[38] VALLS PRIETO, J. *Inteligencia artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 20. The first ones learn with logical rules: "if X is... then Y is..." work very well when the field of action is simple and well defined. To improve their characteristics, expert solutions (also called expert systems) can be added.

[39] ML designs predictive models that build the relation between the variables to be studied by analysing an initial data set, identifying patterns and establishing classification criteria. Once the criteria are set, the AI is able to perform inference when a new data set is introduced. SDPA, *GDPR adequacy of processing incorporating Artificial Intelligence. An introduction*, 2020. Electronic resource obtained via the Web: https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf, [retrieved on 7 November, 2023], p. 6. Moreover, the scope of the system is constructed by itself, not by the human, on the basis of examples extracted from the data to which it has been given access. The ML mechanisms can extract relevant

is part of the field of AI and focuses on the study of computer algorithms that improve automatically through experience[40]. It tries to convert patterns into data to build predictive or explanatory systems, being able to make decisions or detect significant patterns[41]. Thus, it is based on the development of algorithms and technologies that allow the computer mechanism to learn. In addition, it can use those to analyse data, learn through analysis and make decisions or predictions based on learning. ML model testing is performed by validation errors on new data. So the technique is based on an iterative

information from the input data and thus learn to adequately develop the functions for which it was created. SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit., p. 45. In our opinion, the fact that the machine is capable of learning and acting in ways that were not anticipated entails the risk that its actions may lead to unlawful actions.

[40] The algorithm is a "finite succession of operations that are performed in a precise order to give an answer to a problem, perform a computation, process data and carry out other tasks or activities". PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid, 2022, pp. 15-16. There are two types of algorithms: deterministic and non-deterministic. The former are made up of rules whose information is totally defined, so they have the advantage of being more interpretable. On the other hand, the rules of the latter are not completely defined and have the autonomy to process the information and produce new results according to the data entered. The latter are capable of adapting to reality, while being unpredictable because they learn from the data. PALMA ORTIGOSA, A. " El ciclo de vida de los sistemas de Inteligencia Artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos", in Cotino Hueso (Dir.), *Derechos y garantías ante la Inteligencia Artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, p. 32.

ML algorithms do not act in a similar way to traditional algorithms. The former are able to improve themselves automatically through experience and the use of data. To do so, they build a model based on data (training data) that they use in the training phase to make predictions without having been explicitly programmed for that purpose (i.e., algorithms can be created with a given number of images of dogs and cats without the need to define what are the common characteristics of the images of each one. After this first phase, the algorithm is able to autonomously learn the features common to the cat images and will be able to build a model for the recognition of new images, with high accuracy). Not only that, they are also different in terms of the goal they pursue, as ML ones aim to create models that can perform certain actions as predictions. They are generally not transparent, explainable or interpretable, especially when they use neural networks (the operation of which will be discussed briefly below). Traditional algorithms, on the other hand, can be decomposed. ITALIANO, G.F. et al. "L'Intelligenza Artificiale: Dalla ricerca scientifica alle sue applicazioni. Una introduzione di contesto", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 50, 54.

Although AI used to be linked to algorithms, algorithms are not the former, but a part or aspect of it. The former, as procedures susceptible of automatic application, have a wider field of application and cover all computer systems, so that not all algorithms involve AI. However, it is true that every AI includes them, performing some tasks that are directly related to AI functions, from the application of pre-existing knowledge to the realization of forms of learning that contribute to create or modify the model on which the operation of the system in which they are integrated is based. Different algorithms can make up an AIs but these can be seen as a single complex algorithm composed of all the others. SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit., pp. 9-10. Jurisprudence has pronounced on the difference between algorithms and AI. Thus, in Italy, the Consiglio di Stato Sezione III Sentenza 25 novembre 2021, nº. 7891, has established that the former simply refers to a finite sequence of instructions, well defined and unambiguous, so that they can be carried out mechanically and produce a specific result. On the other hand, it defines the latter as systems that perceive their environment and perform actions that maximize the probability of successfully achieving the objectives set.

[41] PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial...*, cit., p. 16. The cited author goes on to point out that, for an ML system to be successful, it must use the appropriate algorithms and carry out a correct management and treatment of the data used for the development of the system.

approach that learns from data, facilitating automation and being able to discover robust patterns[42].

The use of ML is encouraged by the increase in the volume and variety of available data, more powerful analytics, lower storage and analysis costs. Therefore, this technology is strongly linked to data mining, *Big data*[43] and optimization. In this sense, the main elements that make up AI are data and algorithms[44], to which the *hardware*, i.e. the various computer equipment that support the systems[45] is added. The latter are trained with the former to infer certain models, in order to specify the actions required to achieve the desired goal[46]. Thus, the techniques indicated need a database to train the algorithm on how to treat the information[47].

Generally, there are three types of ML depending on the nature of the tasks to be performed by the system: supervised, unsupervised and reinforcement learning. In the first, the algorithm uses training data that has already been adequately pre-labelled by people in the training phase; in the second, algorithms can independently identify patterns and correlations in raw data, i.e., the system learns without receiving instructions, either external or coming from the results of the activity itself. The latter is useful not only

[42] KIM, K.S. & JEONG, Y.H. "A Study on Crime Prediction to Reduce Crime Rate Based on Artificial Intelligence," *Korean Journal of Artificial Intelligence*, vol. 9, no. 1, 2021, p. 16.

[43] Big Data is understood as the union of large amounts of available data and tools capable of analyzing and processing them. HERRERA, F. et al. "Una visión actual de la Inteligencia Artificial: recorrido histórico, datos y aprendizaje, y responsabilidad en el diseño y uso", in Peralta, Salvador Torres y Herrera (Coords.), *El Derecho y la Inteligencia Artificial*, Editorial Universidad de Granada, Granada, 2022, p. 61.

Big Data has been one of the determining factors for the rapid advancement that AI has experienced in recent years. The term refers to large masses of data. It applies to huge data collections that are difficult to deal with using traditional computing technology. They are characterized by three v: huge volume, high velocity and great variety. Other properties are low veracity and high value. Data can be created by people but is generally collected automatically from devices used in the physical world. From a social and legal perspective, what is most relevant with respect to large masses of data, is the possibility to use them for an analytical purpose, i.e. to discover correlations and to make predictions. SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit. p. 12.

Such is the growth of data generation and processing that there is talk of "datification", a phenomenon whereby the aim is to quantify and study any aspect of life in order to transform it into data that, once processed by algorithms, can be used for a wide variety of purposes. MOBILIO, G. "Profilare tramite riconoscimento faciale: il caso de la sicurezza urbana", in Adinolfi and Simoncini (Dirs.), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizione Scientifiche Italiane, Napoli, 2022, p. 183.

[44] There is a synergy between data and AI. The latter is "hungry" for data and this is what has led to its increasingly extensive collection. The availability of large masses of data has favoured new ML applications, so there is synergy between them. In recent decades, data flows have been integrated into a global infrastructure for information processing, centred on the Internet but not limited to it. AI together with Big Data, in combination with the availability of computer sources, have increased the opportunities for profiling individuals, allowing inferences to be made. Subjects can be increasingly monitored, influenced and manipulated on the basis of their own processed and processed personal data. *Ibd*., pp. 63 and 67-68.

[45] DE HOYOS SANCHO, M. "El uso jurisdiccional de los sistemas de Inteligencia Artificial y la necesidad de su armonización en el contexto de la Unión Europea", *Revista General de Derecho Procesal*, nº. 55, 2021, pp. 2-3.

[46] EUROPEAN COMMISSION. *White paper on artificial intelligence. A European approach to excellence and trust*. COM(2020) 65 final, p. 20.

[47] AARVIK, P. *Artificial Intelligence-a promising anti-corruption tool in development settings?*, U4. Anti-corruption Resource Centre, Chr. Michelsen Institute, 2019, p. 1.

because it saves costs when collecting large data sets, but also because it allows AI to identify patterns that humans may not detect. Finally, the third learning modality refers to AIs that learn from feedback from the environment, discovering through trial and error the actions that allow it to "earn" or maximize a given score[48]. They do not need an instructor because they learn from the results of their own actions. In addition to the above, there is a different application such as generative adversarial networks, by means of which a neural network can be trained to generate false data, improving the quality of its products until they cannot be distinguished from real data, and can even deceive another recognition algorithm[49]. The aforementioned categories group different methods that include the aforementioned neural networks, DL, etc.

The latter is linked to ML, or rather can be considered a subcategory of it, and refers to the part of AI that is associated with algorithms inspired by the structure and functions of the brain, i.e. the artificial neural networks[50] that make up that type of learning. These neural networks are computer systems made up of nodes connected by links to which numerical steps are assigned. The architecture is based on the idea of human intelligence based on brain neurons but, in this case, the functioning of each neuron is established by logical-mathematical functions[51]. In order for the neural networks to act, the mechanism must be trained so that it is capable of achieving the objectives it is intended to achieve[52]. These artificial neural networks are multilevel, so they develop deep data processing. They are called deep neural networks because they have a large number of layers in the three basic layers (input, hidden and output). Such networks are capable of building higher levels of abstraction that allow them to solve complex problems such as speech or image recognition[53]. Thus, BROADHURST sees

[48] HAYWARD, K.J. & MAAS, M.M. "Artificial intelligence and crime...", cit. p. 213.

[49] *Idem.* We consider this issue to be particularly relevant with regard to the possible liability for the crimes committed by AIs, because they can be used for the commission of crimes or, as in the latter case, the mechanisms can generate erroneous data *per se*, with the consequences that this entails. Although the issue of criminal liability for offenses committed through AI is very interesting, it is not our task to go into it in depth, since it is far beyond the scope of our study. Therefore, the interested reader is advised to refer to BROADHURST, R. et al. *Artificial Intelligence and Crime...*, cit., pp. 36-39; & KING, T.C. et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", *Science and Engineering Ethics*, vol. 26, nº. 89, 2020, pp. 94 and the next.

[50] On the evolution of artificial neural networks, see extensively, PÉREZ Y MADRID, A. *El reconocimiento facial es un superpoder...*, cit., pp. 19-20. DL is responsible for the current AI boom. Deep neural networks operate as follows: they are an AI technique inspired by the process by which neurons in the biological brain communicate with each other. These networks consist of layers of interconnected digital neurons. Some of them receive an input and others provide an output. Each neuron monitors others in the previous layer and only if enough neurons send it a signal will it send signals to other specific neurons in the next layer. After each general incorrect/correct response to the training data sample, it learns to encode rules to execute its task. HAYWARD, K.J. & MAAS, M.M. "Artificial intelligence and crime...", cit., pp. 212-213.

[51] SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit., p. 56.

[52] ALGERI, L. "Giustizia predittiva: itelligenza artificiale e processo penale", in Adinolfi, A. & Simoncini, A (Dirs.), *Protezione dei dati personali e nuove tecnlogie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizione Scientifiche Italiane, Napoli, 2022, pp. 657-658. The common technique for training a neural network is to provide correct examples, a series of input-output pairs where the latter indicates the appropriate result for the corresponding input. SARTOR, G. *L'intelligenza Artificiale e il Diritto...*, cit., p. 5.

[53] ALGERI, L. "Giustizia predittiva...", cit., p. 662. The author in quotation adds that both types of systems have a common element, the data with which the mechanisms are built and trained.

the study of AI as an attempt to develop a mechanized and simplified version of human neural networks and cognitive processing[54].

In view of what has been explained in this section, it can be concluded that AI is divided into different mechanisms with different functions and ways of acting, depending on the purpose they are intended to achieve.

1.4.Modalities of Artificial Intelligence

In line with the above, it is further inferred that AIs can have different levels of complexity, from simple software installed on a computer to a more complex physical architecture[55] . There is a broad consensus among computational scientists to differentiate between general AI and specific "narrow" AI. VALLS PRIETO makes the distinction between the two, pointing out that the former has to do with conscious beings, eternal life, machines that think like humans or robots that want to control the world. It should possess most of the human cognitive abilities but is currently not available, there is no system that has such capabilities[56]. Thus, he defines it as "the ability to perform tasks that can be performed by a human being and is assumed to have cognitive abilities similar to those that can be found in a human mind"[57]. The second, on the other hand, is a specific and realistic AI. Basically, they are mathematical prediction models that can execute specific human tasks in very specific fields, sometimes with abilities superior to those of people[58]. This type of AI includes image or face recognition.

Another classification distinguishes AI in a tripartite manner according to its abilities and objectives into: weak, medium and strong. The first is linked to systems that are programmed to perform a single task or a combination of tasks in a limited area of expertise, i.e., in a specific domain. Any mechanism for ML, pattern recognition and natural language processing to make autonomous decisions is included in weak AI. Most current systems, as novel as they may be, are designed to perform specific tasks, so they

[54] BROADHURST, R. et al. *Artificial Intelligence and Crime...*, cit., p. 4.

[55] NOVELLI defines the former as generic "AI algorithms" while the latter as "robot agents". NOVELLI, C. *AI and legal personhood: a theoretical survey*, PhD Thesis defended at the University of Bologna, Italy, 2022, p. 25.

[56] VALLS PRIETO, J. *Inteligencia artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 19. Because there is no instrument that has the same capabilities as human beings, CHESTERMAN understands general AI as science fiction at present. CHESTERMAN, S. "Artificial Intelligence and the limits of legal personality", *International and Comparative Law Quarterly*, vol. 69, 2020, p. 821.

[57] VALLS PRIETO, J. *Inteligencia artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 19. DAWES, similarly, understands it as the generalized intelligence that could perform all the cognitive tasks that humans can perform, at least in the way in which the latter do it. Thus, he argues, AI could learn not just something, but anything. For this reason, he is concerned about the future development of these mechanisms, since they could surpass human capabilities. DAWES, J. "Speculative human rights: Artificial Intelligence and the future of humans", *Human Rights Quarterly*, no. 42, 2020, pp. 573-577.

[58] See, extensively, VALLS PRIETO, J. *Inteligencia artificial, Derechos Humanos y bienes jurídicos...*, cit., pp. 19-20. On many occasions both types of AI are confused and, on the other hand, AI can be equated with robotics, when they are different disciplines.

are of this type[59]. Medium AI, also called "Artificial General Intelligence", is the intelligence with which a machine would be able to understand the world like a human and has the ability to perform tasks autonomously. As of today, there are no real-world applications of it; and finally, strong AI (or, Super AI), refers to systems that would not only match, but surpass human intelligence at all levels (i.e., prescribing drugs to patients, creating fantastic literature, etc.)[60]. If the former have no practical application, much less the latter. However, the former does have many real applications in technologies that we use on a daily basis or that impact our daily lives in some way, such as smartphones[61].

Therefore, AIs are configured as a tool for automatic decision making, which are not only used in the private but also in the public sphere, by legal professionals, judges and police officers. Specifically in the criminal law environment, they have been used at different times, from crime prediction in crime prevention (*predictive policing*)[62] to

[59] HAYWARD, K.J. & MAAS, M.M. "Artificial intelligence and crime...", cit., p. 213. The authors go on to point out that weak AI is not without limits and has a number of preconditions for its effective application in a particular domain. They include primarily access to large databases and pragmatic issues related to hardware, human talent and availability of investment. However, both computational and data barriers are falling. Moreover, they do not limit the spread of already capable systems, which is a concern in many criminal contexts. At the same time, when all the preconditions are in place, current AIs present problems known as "artificial stupidity." They put forward three reasons for making such a claim. First, AIs are often prone to catastrophic forgetting, i.e., inability to easily transfer learning from one context to another; second, AIs are susceptible to adversarial input, i.e., data designed to alter the way the system processes stimuli; and third, AIs do not have "adversarial input", i.e., data designed to alter the way the system processes stimuli; furthermore, AIs do not have "common sense" and thus, contrary to some of the connotations in the "intelligent" world, inevitably suffer from the "Garbage-in, Garbage-out" problem, which can lead to problems with biases. Finally, the problem of unpredictable autonomy, since the AI may act unexpectedly when confronted with novel situations.

[60] BROADHURST, R. et al. *Artificial Intelligence and Crime...*, cit., pp. 4-5. The authors argue that strong AI could lead to a quantum leap of self-improvement, called "Sigularity", where each improvement in the cycle would produce better machines. This could have numerous benefits, although the devastating impact on our environment is emphasized.

[61] Some of these applications include speech recognition, computer vision, extended reality, gaming and natural language processing. BROADHURST, R. et al. *Artificial Intelligence and Crime...*, cit., pp. 8-9.

[62] The use of AI is becoming increasingly important in policing and in the role of predicting crime trends or mapping potential hot spots. What characterizes predictive policing is the use of large amounts of historical data analyzed with quantitative techniques to estimate from algorithms an unknown value, the results of which will help to manage police resources more effectively to increase public safety and reduce crime. The main challenge of this technique lies in data collection and subsequent analysis. TORRES LÓPEZ, L.S. & PERALTA GUTIÉRREZ, A. "Uso policial de sistemas de inteligencia artificial en el ámbito comparado", in Peralta et al. (Coords.), *El Derecho y la Inteligencia Artificial*, EUG, Granada, 2022, pp. 453-473. The authors make a broad overview of different techniques developed in different countries. On the subject, see also ALONSO SALGADO, C. "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *Ius et Scientia*, vol. 7, nº. 1, 2021, pp. 25-36; and ALGERI, L. "Giustizia predittiva...", cit., pp. 663-667. Currently, in the field of law enforcement, predictive policing techniques are being developed on a large scale to predict the commission of crime and its location, as well as in individual profiling. There are two categories of predictive policing software. On the one hand, there is the tendency to identify hotspots or places where certain crimes are most likely to be committed and, on the other, crime linking, which consists of following the criminal patterns of certain individuals to predict where and when they will commit the next one.

They are also very useful in the prevention of specific types of crime such as corruption. See, in this sense, DOMINGO JARAMILLO, C. "Aproximación a la aplicación de sistemas de inteligencia artificial para prevenir la corrupción en la administración pública", *Cuadernos de Política Criminal*, nº. 140, 2023, pp. 105-134.

sentencing[63], among others such as decision making on the calculation of the probability of recidivism. They have also been implemented in the area of public safety maintenance or law enforcement by law enforcement officers, who make use, among other techniques, of biometric data for remote recognition of known or suspected criminals who have committed a serious crime, in order to avoid disrupting public safety. It is on this last issue that the present research focuses, as there are many controversies and problems involved, especially with regard to the protection of fundamental rights and freedoms.

2. Biometrics and biometric data

The logical development of the research leads us to address at this point what is meant by biometrics and biometric data, as well as biometric identification systems, insofar as the mechanisms that are the subject of our study, as we will have the opportunity to explain in more detail in the next section, consist of the automated identification of an individual through a physical characteristic, in this case, the face.

2.1.What is biometrics

Although automated person recognition systems emerged in the early 1960s, the use of the term biometrics in this sense began two decades later; in the 1970s it was called "automated personal identification" (API)[64]. The word biometrics is composed of two elements. On the one hand, we find the notion bio (life)[65] and, on the other, metrics or measurability, referring to the mechanical processing of these characteristics[66]. In this line, it is understood that only living beings present these very specific qualities, unique

[63] In fact, on January 30, 2023, the first sentence using ChatGPT was issued in the Colombian Constitutional Court. The judge in charge of the case entered into the system several questions that the mechanism answered. The magistrate used the results to support the outcome of the ruling. He ruled in favour of a mother so that her autistic son would be exempted from paying for medical appointments, therapies and transportation to hospital centres because the family did not have sufficient economic resources to do so.

ChatGPT was designed by a private company but there are also applications developed by public entities. In Argentina, the Public Prosecutor's Office of the City of Buenos Aires has adopted the *Prometea* system, which issues judicial resolutions in less than fifteen seconds with a 98% accuracy rate. To learn more about it, see CORVALÁN, J.G. "La primera inteligencia artificial predictiva al servicio de la justicia: *Prometea*", *La Ley*, nº. 186, 2017.

[64] WAYMAN, J.L. "The scientific development of biometrics over the last 40 years", *The History of Information Security: A Comprehensive Handbook*, Elsevier Science B.V., 2007, p. 263. The author further notes that prior to 1970 there seemed to be little awareness of the existence of a general field of study, with distinct techniques existing separately.

[65] From a philosophical perspective, the problem of measuring life is not a trivial matter. For GHILARDI/KELLER, the specific problem of biometry is the unit of measurement of life. They recognize that the action of measuring the latter is rather to measure some of its quantitative aspects. GHILARDI, G. & KELLER, F. "Epistemological Foundation of Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 26.

[66] MORDINI, E. et al. "Introduction", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 8.

and stable enough to be used as identifiers. Specifically, it is currently linked to the automated recognition of individuals by their behavioural or physical properties[67]. For this technology to be considered automatic, it must recognize or verify a characteristic in a reasonable time and without a high level of human involvement[68].

Today we are faced with a restricted or limited term for biometry, far removed from its original meaning, given that it previously referred to studies that sought to contribute to biological knowledge by establishing continuous variables[69]. Thus, the objective of the biometric science of our days is to determine metrically the singularity of a subject in relation to a set and allow its indubitable recognition[70]. As ALBRIZIO points out, biometrics is the history of the encounter between life sciences and measurement. It thus encompasses quantitative research on man, animals and plants. It uses measurements, instruments, mathematics and statistics[71], so that data of this type is the result of procedures aimed at measuring the uniqueness of a characteristic, anatomical or behavioural, of a subject or a group[72].

Although we are aware of the extent of the term, for the purposes of our study, we will use it in the sense in which it is currently used, i.e., restricted[73]. Thus, following HOPKINS, we understand biometrics as the application of computational methods to biological characteristics, especially the study of the biological characteristics of humans[74]. This technique makes it possible to authenticate identities and relate them to events, locations, groups and concepts of interest[75].

---

[67] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales*, Aranzadi, Navarra, 2017, p. 44. The availability of biometric identification systems has increased in recent decades due to significant advances in the field of computer processing. GHILARDI, G. & KELLER, F. "Epistemological Foundation of Biometrics...", cit. p. 24.

[68] RIERA, A. et al. "Electrophysiological Biometrics: Opportunities and Risks", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 152.

[69] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales*…, cit., p. 44.

[70] *Ibd.*, p. 49.

[71] ALBRIZIO, A. "Biometry and Anthropometry: from Galton to Constitutional Medicine", *Journal of Anthropological Sciences*, vol. 85, 2007, p. 102. For more on the history of biometry, see pp. 103-106 of the same work.

[72] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., p. 27.

[73] Similarly, WAYMAN, J.L. "The scientific development of biometrics over the last 40 years...", cit., p. 263.

[74] HOPKINS, R. "An Introduction to Biometrics and Large Scale Civilian Identification," *International Review of Law, Computers & Technology*, vol. 13, no. 3, 2010, p. 337.

[75] ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed and you've been found suspicious. Biometrics and data protection in criminal justice processing", in Leenes, R. et al. (Dirs.), *Data protection and privacy. The internet of bodies, vol. II*, Hart Publishing, 2018, p. 2.

2.2.Biometric data

Before addressing the types of biometric data, it is necessary to distinguish them from biometrics since they are two different concepts but are usually used as synonyms. On the one hand, the notion of biometric data is technical and legal, while the second is only technical and derived from the field of biometric recognition. Therefore, in the context of data protection and, following the definition above, it should be understood as the automatic method of recognition based on biometric characteristics. The term biometric data, on the other hand, includes the transformation of such elements into formats that can be used for recognition[76].

Biometric recognition procedures or techniques are of very different types[77] and, depending on the characteristics to be measured (iris, retina, DNA, fingerprints, face, etc.), biometric data can be divided into two broad categories: static and dynamic. The former are linked to the anatomical-physical aspects of individuals, which are unique and permanent and their presence is considered almost univocally united to a given subject. These include fingerprints, hand geometry, iris, retina and face. Because of these characteristics, they are called "strong biometrics"[78]. From all of them, a sample is taken at a given time and, subsequently, a measurement study is performed from which the biometric data or pattern is obtained as a result.

Dynamic biometrics (or weak biometrics) are more complex than the previous ones and are obtained from physiological characteristics, i.e., they do not correspond to a physical trait or element. They are less unique or stable and can be used for identification purposes if not in isolation, since they can only partially determine the identity of an individual. For this reason, they should only be used in concrete spatio-temporal contexts or linked to other similar data, which can offer greater discriminating power for authentication, identification of subjects in small groups and monitoring of individual identities in a limited period of time[79]. The two main sources of such information are data obtained from motor skills and body signals and parameters. This category includes dynamic signature, voice, movement of the body (or a part of it) while performing an activity, typing, and body signals such as breathing rate or agitation response to certain stimuli, etc.[80].

---

[76] JASSERAND, C. "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data", *European Data Protection Law Review*, vol. 2, 2016, p. 301.

[77] SHARIF, M. et al. "An Overview of Biometrics Methods", in Singh, A.K. & Mohan, A. (Eds.), *Handbook of Multimedia Information Security: Techniques and Applications*, Springer, 2019, pp. 16-30. The authors make a broad classification between biological and behavioural biometrics. The first is further subdivided into: a) visual (those that can be seen through the human eyes: iris, retina, face, ear, nails, footprint and dynamics); b) chemical, which is identified with DNA; c) olfactory, linked to body odour; d) spatial (hand and lip geometry); and e) others such as blood vessel patterns, sweat pore analysis, etc. Within the second include the following: a) signature; b) auditory biometrics: voice, breathing and lip movement; c) keystroke dynamics; d) gait style; and e) the grip or holding capacity of a hand.

[78] MORDINI, E. et al. "Introduction...", cit., p. 8.

[79] *Ibd.*, p. 9.

[80] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., pp. 53-55.

In addition to the above, there is a third category called soft biometrics, which refers to generic characteristics that cannot be linked to a particular individual. More specifically, following NIXON *et al*. we understand that they could be defined as "the estimation or use of personal characteristics describable by humans that can be used to aid or effect person recognition"[81]. Among the elements that the techniques included in this category aim to measure are gender, age, race and ethnicity, weight, size, etc. They can be very useful to reinforce the two previous ones, as they allow to reduce the number of possibilities and, consequently, to refine the identification process[82]. Putting all the above together, it can be stated that biometric data allow the unique recognition of an individual from his or her own physical or behavioural traits.

This is because each human being acquires these characteristics in a particular way. Therefore, in its various manifestations or forms, biometrics is the most reliable method for authentication in a secure manner[83]. This is also due to the fact that conventional identification systems based on the possession of identity cards or some kind of alphanumeric combination, such as a social security number or password, are not entirely reliable, since they can be lost or forgotten[84].

Thus, in view of all that has been indicated so far, we can affirm that biometric elements constitute a type of information about a natural person, whether identified or identifiable, and therefore constitute a category of personal data[85]. The first form of identification would be that in which the person, within a group, can be distinguished from its other members[86]. For its part, the identity of the identifiable subject can be determined, directly or indirectly, by means of an identifier, such as name, identification number, location data, online identifier or by the elements of physical, physiological, genetic, psychological, economic, cultural or social identity[87]; that is, he or she has not yet been identified but it is possible to do so through his or her biometric data.

---

[81] NIXON, M.S. et al. "On soft biometrics," *Pattern Recognition Letters*, vol. 68, 2015, p. 220.

[82] MORDINI, E. et al. "Introduction...", cit., p. 9; VAN DER PLOEG, I. "The body as data in the age of information", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 179, 182.

[83] SHARIF, M. et al. "An Overview of Biometrics Methods...", cit., p. 15.

[84] PANKANTI, S. BOLLE, R.M. & JAIN, A. "Biometrics: The Future of Identification [guest editors' introduction]", *Computer*, vol. 33, nº. 2, 2000, p. 46; RATHA, N.K. et al. "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, vol. 40, no. 3, 2001, p. 629. The latter authors understand that the change from traditional systems to biometrics may also entail some problems, since the fact that it is immutable means that, if the information is compromised, its replacement is not possible.

[85] Personal data is information of any kind, so the term includes both sensitive data and other more general categories. It need not be contained in a database or structured file. Opinion 4/2007 on the concept of personal data of the Article 29 Working Party, 20 June 2007, pp. 6 and next. The Working Group establishes four main criteria into which the definition of personal data is divided: a) any information, b) about, c) identified or identifiable person; and d) natural person.

[86] SHARIF, M. et al. "An Overview of Biometrics Methods...," cit., p. 13.

[87] See the definition of personal data set out in Art. 3(1) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA (hereinafter Law Enforcement Directive, LED).

More specifically, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive, hereinafter LED), when it raises the definition of biometric data in its art. 3.13), it specifies that they are a type of personal data obtained through specific technical processing, "relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"[88].

Biometric data have some essential characteristics: they are universal, which means that they are shared by all human beings; they are unique to each person and invariable throughout life[89]. In addition to the above, we must add an essential one, which is collectability, i.e., that the characteristic can be measured quantitatively[90]. For all these reasons, using biometric data, it is possible to univocally recognize or identify an individual.

2.3.Differentiating biometric identification from emotion detection and biometric categorization

Initially, biometrics was mainly used for identification purposes, but it is now extending to other areas such as gender and race determination through the identification of parameters such as voice, gait or handwriting. These are included in the aforementioned weak biometrics and are becoming increasingly important for profiling,

[88] Identical definition of biometric data is also found in Art. 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 17 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR); Art. 3.18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC; and in Art. 3(34) AIA.

[89] COTINO HUESO, L. "Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection", in Balaguer, Callejón, F. & Cotino Hueso, L. (Coords.), *Derecho Público de la Inteligencia Artificial*, Fundación Manuel Jiménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, p. 353.

CLARK in 1994 established a broader list of characteristics that biometric data must have. Thus, they must be: 1) universal, 2) unique, 3) permanent, 4) essential (natural characteristic of the person, which he maintains and preserves), 5) collectable, 6) storable, 7) exclusive, 8) accurate, 9) simple, 10) reasonable cost, 11) convenient, in the sense that measuring and storing them should not be inconvenient or time-consuming, and 12) acceptable (in accordance with social standards). CLARK, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues", *Information Technology & People*, no. 7-4, 1994, pp. 7-8.

[90] JAIN, A.K. et al. "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 2004, p. 4.

emotion recognition and people categorization[91]. The first one, as its name suggests, is understood as the system that makes it possible to distinguish or infer emotions or intentions of natural persons by means of their biometric data (art 3.39) AIA). Through this type of mechanism, intentions can also be deduced and do not include certain physical states such as pain or tiredness, nor does it detect obvious expressions, gestures or movements unless they can be used to distinguish or deduce emotions (recital 18 AIA)[92].

On the other hand, a biometric categorization system, as stated in art. 3(40) AIA, is any AI mechanism aimed at including natural persons in specific categories on the basis of their biometric data. Such categories, as stated in recital 16 AIA, may refer to sex, age, hair colour, eye color, tattoos, behavioural or personality traits, language, religion, membership of a national minority or sexual or political orientation[93]. Recital 30 prohibits the use of these mechanisms when parameters such as an individual's face or fingerprints are used for the purpose of inferring political opinions, union membership, religious or philosophical convictions, race, life or sexual orientation. However, this prohibition does not extend to other functions such as the classification of images according to hair or eye colour that may be used in the field of law enforcement, when the lawful labelling, filtering and categorization of the data were obtained in accordance with national or Union law.

On the other hand, other types of biometric identifiers such as fingerprints, DNA, face, etc., are used for the task of identification in first generation technologies, qualified as "robust" and refer to recognition methods that are based on primary biometric attributes, i.e., those that sufficiently combine the qualities of uniqueness and permanence. Both types of data do not act in isolation and can complement each other[94],

[91] The need to identify people arose centuries ago and has evolved with the various revolutions that have occurred throughout history. Initially, this was done using instruments or parameters that we could call traditional. However, in the current era of globalization, new techniques have emerged that measure not only physical characteristics but also physiological and behavioural ones. On this aspect, see extensively, MORDINI, E. et al. "Introduction...", cit., pp. 1-19; FAIRHURST, M. et al. "Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data", *IET Biometrics*, vol. 6, nº. 6, 2017, pp. 369-378.

[92] Although systems based on facial emotion detection are used in the police and judicial field, such as police lie detection and polygraphs, also entailing serious damage to the rights and freedoms of the population, our study will focus specifically on the detection of facial parameters for remote identification of individuals, since this technique of emotion detection (closely linked to the one that is the focus of our research), due to its particular characteristics and complexity, requires a detailed and independent analysis. However, to learn more about it and all the issues that revolve around it, see in greater depth, NERONI REZENDE, I. *Surveillance Risks in IoT applied to Smart cities*, PhD thesis defended in 2023 at the University of Bologna, Italy, pp. 217-236.

[93] This category excludes biometric categorization systems that are an accessory feature intrinsically linked to another commercial service. This means that such a feature cannot be used, for objective technical reasons, without the main service and that the integration of such a feature or functionality is not a means to circumvent the applicability of the AIA rules. Filters used in social networking services that classify facial or body features so that users can add or modify images or videos could be considered an accessory feature, because such filters cannot be used without the main service of social networking, which consists of sharing content online.

[94] The combined use of several biometric techniques overcomes some of the limitations imposed by systems that use only one biometric technique. These systems are known as "multimodal biometrics systems" and are expected to be more reliable due to the presence of several independent pieces of evidence. This type of mechanism addresses the problem of non-universality, as multiple traits ensure sufficient

since the former have a great potential to support the latter, as well as in identification systems that do not pretend to be indubitable, but reasonable in a given context[95].

Along these lines, by going beyond the mere personal identification with these techniques, the broader concept of biometric-based data was proposed in Amendment No. 21 of 2023 to the Proposed Regulation (although it did not see the light of day in the final version of June 2024), which referred to data based on biometric techniques. This was understood as new data resulting from specific technical processing of an individual's physical, physiological or behavioural signals. It included facial expressions, movements, heart rate, voice, keystrokes or gait, which in some cases make it possible to identify or confirm the unique identification of a natural person[96].

2.4.Functions of biometric systems: identification and identity verification

Having exposed the term biometrics, the definition of biometric data and the distinction of identification from other tasks such as emotion detection and biometric categorization, it necessary to indicate what biometric recognition is and its various manifestations or ways of being used, being a general term used to cover the functions of a biometric system that uses data of this type, i.e. those of identification and verification[97]. The former is defined in recital 15 of the AIA, which follows the provisions of the GDPR and the LED. Thus, we are dealing with a form of automated recognition of physical, physiological or behavioural human characteristics, including face, eye movement, body shape, voice, intonation, gait, posture, heart rate, blood pressure, smell or keystrokes, with the aim of determining the identity of an individual by comparing his or her biometric data with those of other persons stored in a reference database, regardless of whether or not the person has given consent.

It goes on to differentiate between identification and verification. The latter is outside the former and comprises authentication, the sole purpose of which is to confirm that a particular person is who he or she claims to be, as well as the identity of that person in order for him or her to access a service, unlock a device or securely access premises.

Thus, while biometric identification is normally one-to-many, verification is one-to-one and involves automated verification including authentication of identity through

population coverage. In addition, they provide measures against impersonation because of the difficulty involved in simultaneously impersonating several traits of a user. JAIN, A.K. et al. "An Introduction to Biometric Recognition...", cit., pp. 14-15. The fusion of methods is not always trivial and the objective of combining several systems is to increase security. SERRATOSA, F. *La biometría para la identificación de personas*, Universitat Oberta de Catalunya, Barcelona, 2008, p. 5.

[95] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., pp. 105-107.

[96] P9_TA(2023)0236. Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

[97] JASSERAND, C. "Legal Nature of Biometric Data...", cit. p. 299.

comparison of biometric data with others that have been previously provided (art. 3.36) AIA). In this case, to give an example, it would be the function of unlocking and accessing a Smartphone or any other similar device with the biometric data provided by the user of the system.

There are, as can be seen, important differences between the task of identification and that of verification[98]. The former involves determining the identity of an individual by comparing his biometric data with all the data contained in a database, even though there may be no consent to do so and the owner of the data may not even be aware that the data is being processed. On the other hand, verification consists of establishing that a person is who he or she says he or she is through the comparison of his or her biometric data with those previously provided even by him or herself, so that there is consent in the processing of his or her biometric information. In this last point lies what we consider to be the main difference, or at least the most important difference, between the two uses of biometric identification systems. This is because in the former there is no consent to the processing of personal data, which can lead to issues regarding its consideration as lawful or not.

Moreover, an important issue with respect to biometric data which use is aimed at unequivocally identifying a person is that they are considered a special category of personal data according to art. 10 LED and, therefore, sensitive (moreover, the aforementioned precept prohibits their processing when they are intended to univocally identify a natural person, except in certain cases). On the other hand, if they are not linked to such purpose, they do not acquire such status[99]. In our specific case, the image of the face, being the most visible and identifiable personal data of individuals, is included in the category of sensitive data and, therefore, special. Even more so when the FR techniques in our field of study have the ultimate aim of identifying individuals for law enforcement purposes, since the decisions taken after personal detection have repercussions and serious consequences on the rights and freedoms of the subject in question. In this sense, art. 3.38) AIA establishes the concept of sensitive operational data, such as those linked to activities of prevention, detection, investigation or prosecution of crimes whose disclosure could jeopardize the integrity of criminal cases.

Finally, to conclude this section, it should be noted that technological advances have led to biometrics through algorithmic data processing, understood as scoring and classification instruments that contribute to the accumulation of symbolic and intangible capital that in turn shape the cultural and economic position in society[100]. Caution should

[98] Despite the differences, some authors confuse them. For example, MITCHELL, when stating the purpose of biometrics, identifies it as the measurement of a unique, personal, physical or behavioural characteristic to verify the identity of a subject. He goes on to point out that biometric systems can be used as a tool to determine whether one belongs to a group with certain rights or is denied privileges or benefits. MITCHELL, A. "Distinguishing friend from foe: Law and policy in the age of battlefield biometrics", *The Canadian yearbook of International Law*, vol. 50, 2012, p. 291.

[99] COTINO HUESO, L. " Reconocimiento facial automatizado y sistemas de identificación biométrica...", cit., p. 354. The author is surprised that data revealing emotions, thoughts and intentions are not among the special categories of data.

[100] JANSEN, F. et al. "Biometric identity systems in law enforcement...," cit., p. 4.

be exercised when implementing systems such as the one at the center of the research, since biometric identification mechanisms are based on social relations that establish who has the power to use them and in what situations, being especially dangerous in the police and law enforcement sphere. In addition, there is a risk of deriving in a state of ubiquitous and continuous surveillance of citizens, intolerable in a Social and democratic state governed by the rule of law. Let us now turn to remote biometric identification systems and, more specifically, those based on the detection of facial characteristics, namely FRs.

3. Remote biometric identification systems especially facial recognition

Having studied the term AI as well as biometric data and biometrics, with their different functions and utilities, it is necessary to analyse RBIS and, more specifically, the facial recognition technique, which is the specific objective of our research when used in public places for law enforcement purposes.

Along similar lines, the AIA, although it does not expressly refer to FR mechanisms, in its art. 3.41) defines RBIS as "an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database"[101]. Definition that can be extrapolated to FRs. Therefore, some conclusions can be drawn from the above. We are dealing with an AIs that, as its name indicates, makes it possible to identify individuals through their biometric information[102], by their bodily attributes, in this particular case, their face, using DL techniques[103]. Thus, FR-based technology allows images to be developed and interpreted and is one of the most popular biometrics. It can be used to identify or authenticate an individual through the characteristics of the face, which is the personal data par excellence, as it is particularly visible and easy to recognize, whether in physical or digital space[104].

One of the advantages of this technique is that it allows to recognize individuals remotely through the recordings extracted from video or CCTV cameras in a subtle way instead of waiting for their intervention, for example, by placing their hand or fingerprint on a scanner or by placing the eye on the exact place where the iris reader is located. Thus, it can be put into operation in an unobtrusive way, which makes it particularly

[101] The previous 2021 proposal included the fact that the system implementer does not know in advance whether the person in question is in that database and will be able to be identified, which is not foreseen in the final 2024 version.

[102] COTINO HUESO, L., " Reconocimiento facial automatizado y sistemas de identificación biométrica...", cit., pp. 352-353.

[103] As will be discussed in greater depth in the corresponding section of Chapter II of this study, other techniques have been used previously for facial recognition, although DL is currently the dominant technique for facial detection and analysis. MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU*, European Parliamentary Research Service, Brussels, 2021, p. 2.

[104] COLACURI, M., "Riconoscimento faciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini", in Balbi, G., et al, (Dirs.), *Diritto penale e intelligenza artificiale "nuovi scenari"*, G. Giappichelli Editore, Torino, 2022, pp. 120-121.

suitable for surveillance applications[105], crime prevention and control. In this way, people can be completely unaware of its existence and not feel under observation[106]. This is also one of the risks of such mechanisms, since they can be used without the knowledge and, of course, without the consent of the individuals under surveillance, which leads to serious controversies about the appropriateness of their implementation due to issues such as the infringement of rights and freedoms as well as other problems related to the design and implementation.

As mentioned above, these systems do not include those for verification, which is justified in recital 17 of the AIA by the fact that the latter are considered to have a lesser impact on rights, since data processing is not carried out with a large number of persons without their active participation, but identification is normally carried out one-to-one and with the knowledge of the subject involved.

3.1.Ways in which FRs operate

In the case of FRs, the way in which they operate must be indicated. These mechanisms must be trained to be able to compare and identify images of faces. To this end, the starting point is the collection of a data set, which should be as large as possible, appropriately catalogued and labelled. The process of learning and continuous improvement of the machine arises through the techniques of inductive correlation and probabilistic inference based on the statistical frequency with which certain schemes are replicated in the sample. Once the images are presented to the camera, an algorithm (learner) comes into play that guides the learning from the labelled data and, in turn, informs a subsequent algorithm (classifier) about the modalities with which to individualize the relationships behind the new expected input and output[107]. Given the rapid increase in the use of FRs, their training has become a critical issue. To assess the way in which this has been done, some metrics have been developed: *False Match Rate (FMR),* or percentage of intruder samples that are incorrectly recognized as the claimed identity; *False Non-Match Rate (FNMR)*: percentage of genuine samples that are incorrectly rejected; *Accuracy*: percentage of samples correctly classified; *Genuine Accept Rate (GAR)*: percentage of genuine samples that are correctly accepted; *Detection Rate*: percentage of properly detected intruders; *Equal Error Rate (EER)*: error rate where FMR and FNMR are equal; and *The Receiver Operating Characteristics (ROC) Curve*, which is the plot of FRR versus FAR obtained from different detection threshold values. It can also be obtained by plotting TAR against FAR. The area under the ROC Curve (AUROC) is the metric representing system training, which takes the values between 0.5 and 1[108].

[105] TASKIRAN, M. et al. "Face recognition...", cit., p. 1.
[106] SHARIF, M. et al. "An Overview of Biometrics Methods...", cit., pp. 19-20.
[107] COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit., p. 128.
[108] TASKIRAN, M. et al. "Face recognition...", cit., p. 4.

Once the mechanisms have been trained to recognize faces, they operate in six main stages:

1) Acquisition of the input image or video of the face. Face detection consists of estimating the bounding box of the face in an image or video frames. This process should be robust to differences in pose, illumination and scale, and should eliminate the background as much as possible;
2) The facial anti-spoofing module ensures system security through the use of presentation or attack detection. In this regard, it should be noted that one of the biggest problems of the FR is its vulnerability to spoofing attacks using photographs, videos or 3D masks. They are most common during biometric data enrolment, feature extraction or the decision phase. Anti-impersonation in FR can be done by detecting physiological movements such as blinking, changes in facial expression, mouth or head movements[109];
3) Detection of the face and/or face lines in the image of each video frame. Once the face is detected, the facial lines can be used for face alignment. This task has been substantially improved by recent advances in DL techniques. There are some approaches that have coupled different techniques such as face and face line detection with others such as gender recognition;
4) Image or video pre-processing, which may consist of alignment, frame selection, noise reduction, contrast enhancement or similar operations;
5) Image or video facial feature extraction. Methods using images use holistic, model or texture-based feature extraction approaches, while those using videos use sets or sequences;
6) Facial identification or verification[110]. In this last phase, a specific image is compared with the database containing all the stored templates to find the closest match and thus obtain the identity of the subject in question[111]. Once this has been done, the mechanism issues a score in terms of probability of coincidence of the person with one of the images contained in the database, and it is up to the person in charge of the mechanism to assess whether or not it really corresponds to the subject to be identified.

3.2.Definition of facial recognition systems

Simplifying what has been said so far, FRs can be understood as a technical AI procedure to assess whether two facial images represent the same person. The system is based on the comparison of two sources of information. On the one hand, the database containing the biometric information of the face of a series of facial images of identified

[109] Techniques based on DL and neural networks are used in this area. But spoofing is not the only problem with FRs, as there are also other attacks on the network or the database where the biometric information is stored. *Ibd.*, pp. 6-7.

[110] *Ibd.*, pp. 3-4.

[111] PÉREZ Y MADRID, A. *Facial recognition es un superpoder*, cit., p. 25.

persons (depending on the context and the purpose for which the AI is used, the database may consist of all the images in the possession of the police force, when the system is used in routine investigation processes, or of images of a limited number of selected individuals, with which a watch or watch list is compiled, when the mechanism is used for specific events in real time); and, on the other hand, images of unidentified individuals, from which facial biometric data are extracted by a computer program. The sources from which the images originate are diverse. They can be obtained, for example, from LEAs recordings or from private surveillance systems and subsequently processed in police facilities for that purpose, and those obtained and processed in real time by CCTV at an event where this AI technique is being applied. Once both sources of information are available, the system compares them and scores the similarity of the faces, thus informing of a possible match[112].

Thus, FRs are biometric identification systems[113] capable of capturing in milliseconds the image of an individual, generating a template and comparing it, for example, with templates of people wanted by the police; or, they can also automatically generate large amounts of processed data that can be used for many different purposes, including the maintenance of public safety[114].

Within the scope of the latter, following what is established in the AIA in art. 3.42) and 43), two types of remote biometric identification systems are distinguished and, therefore, of FR. Those that act "in real time" or "delayed", respectively. In the former,

[112] IZQUIERDO CARRASCO, M. "La utilización policial de los sistemas de reconocimiento facial automático", *Ius et Veritas*, nº. 60, 2020, p. 88. The author sets out the definition used in the Judgment of the High Court of Justice, Queen's Bench Division, Divisional court. Case CO/4085/2018, Bridges versus CCSWP (Chief Constable of South Wales Police) and SSHD (Secretary of State for the Home Department).

[113] Information Security Observatory. *Study on biometric technologies applied to security*, Ministry of Industry, Tourism and Trade, 2011, p. 22; and National Institute of Cybersecurity (INCIBE). *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario*, Spain, 2016, p.4. The use of biometrics in police matters is not a novel issue, since the analysis of the physical characteristics of individuals has been used to identify them since ancient times. Until electronic methods of identification were developed, this was done manually. See, COFFIN, J.S. & INGRAM, D. *Facial recognition system for security Access and identification,* United States Patent, Nº. 5,991,429, Washington DC: United States Patent and Trademark Office, 1999, p. 11; & DÍAZ RODRÍGUEZ, V. "Sistemas biométricos en materia criminal: un estudio comparado", *Revista del Instituto de Ciencias Jurídicas de Puebla*, nº. 31, 2013, pp. 30-34. Specifically, the use of photographs for the identification of suspects is an old element of police investigation. Current (automated) facial recognition is an extension of traditional methods used in justice systems since the 19th century. In this regard, MANN, M. & SMITH, M. "Automated Facial Recognition technology: recent developments and approaches to oversight", *University of New South Wales Law Journal*, vol. 40, nº.1, 2017, p. 122.

There are those who also understand, establishing a broad concept of FRs, which we are dealing with a categorization system and not an identification system because today the application of the technique for identity verification extends beyond the latter function and includes the intricate process of differentiating between genuine and fraudulent attempts at identity representation. In addition, the systems are not only capable of detecting facial features but can interpret expressions and emotions, adding further complexity and utility to the identity verification process. HAMZAH, M.A. "Advancing personal identity verification by integrating facial recognition through deep learning algorithms", *International Journal of information Technology*, 2024, p. 1. The author proposes a FRs based on the CNN technique. However, by limiting our object of study to identification through face parameters and leaving aside, for example, verification and emotion detection, we understand them as identification systems.

[114] COTINO HUESO, L. "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial...", cit., p. 4.

biometric data collection, matching and identification are performed without significant delay. It includes not only instantaneous identification but also identification performed with limited minimal delays; while the delayed system is any system that does not perform the above actions "in real time". Both have different characteristics, are used in different ways and the risks they present are not considered to be the same either. For this reason, the latter is regarded as an intolerable risk and is therefore prohibited except in specific situations. On the other hand, those who act in a deferred manner are considered to be high risk and must observe the provisions of the AIA. All this will be analysed in greater depth below in the corresponding sections of this research.

FRs are used especially in investigative work, as part of many security and observation systems in areas such as international identification, identity cards, live recognition, etc. These mechanisms, because they deal with such sensitive personal data as images of an individual's face, can seriously jeopardize fundamental rights, especially the protection of personal data and privacy. Added to this is the way in which the information with which the system is trained is collected, since on many occasions it is obtained without the knowledge or consent of the owner, as is the case, for example, with data captured through the Internet or social networks.

Although FRs are used to perform a multitude of tasks in both the public and private spheres, we will focus on the former and, more specifically, on law enforcement by the agents entrusted with this mission to ensure public safety; and, more specifically, in uncontrolled places such as streets, squares, etc., because in these, the mechanisms are likely to identify an indeterminate number of individuals and lead to situations of mass surveillance. We leave aside other areas or activities such as border control, airports or critical infrastructures, as each of these scenarios requires an independent and detailed analysis due to their specific characteristics.

II. NEW CHALLENGES POSSED BY CRIME THAT MERIT THE ADOPTION OF NEW CONTROL MESURES

Once the basic concepts on which much of our research is based have been exposed, it is time to approach the new challenges that crime brings with it in today's society, which seriously endanger security and generate great social alarm. Hence, the adoption of novel measures –some of them even restrictive of fundamental rights and freedoms– to guarantee the adequate maintenance of citizen security by the agents entrusted with this mission, This is the case with AIs in general and FRs with the aim of guaranteeing compliance with the Law, in particular.

In today's global society there are a series of emerging threats and risks that endanger the security of citizens. These problems must be addressed in a coherent and effective manner, which is why security is a priority element on the public agenda. To give just one example, since 2013 there has been a National Security Strategy (hereinafter, NSS) in Spain and a National Security Law (Law 36/2015, of September 28), whose

Preamble defines security as "the basis on which a society can develop, preserve its freedom and the prosperity of its citizens, and guarantee the stability and proper functioning of its institutions"[115]. It also states that the actors and circumstances that endanger security levels are subject to constant mutation, and that it is the responsibility of the public authorities to equip themselves with the regulations, procedures and resources that will enable them to respond effectively to these security challenges.

The latter is particularly threatened by crime, although current risks are characterized by heterogeneity and constant change, especially due to the advance of new technologies and jihadist terrorism. Thus, among the risks and threats to national security (which can be transferred *mutatis mutandi* to the field of public security), the NSS highlights terrorism and violent radicalization, cybercrime, threats to critical infrastructures, as well as organized crime and serious crime[116]. To the above we add, for the purposes of our study, public disorder that may endanger the life or physical integrity of individuals.

Of particular concern is terrorism, which, following the attacks of September 11, 2001, has gone from being considered an internal problem specific to each country to a global one. This criminal manifestation has evolved, thanks to globalization and ICT, towards internationalization, and has moved away from political objectives to become identified with religious fundamentalism. Thus, as GODOY points out, Islamic radicalism in its different forms is the main threat to today's society[117]. This new

[115] Likewise, Article 3 defines national security as "the action of the State aimed at protecting the freedom, rights and welfare of citizens, guaranteeing the defence of Spain and its constitutional principles and values, as well as contributing, together with our partners and allies, to international security in the fulfilment of the commitments assumed". This conceptualization has been criticized by part of the doctrine, inasmuch as some authors understand that defining it as an action is only accurate when it is in an ideal State. See, in this sense, JAIME, O. et al. "Aproximación a la seguridad nacional", in De la Corte Ibáñez, L. & Blanco Navarro, J.M. (Dirs.), *Seguridad Nacional, Amenazas y Respuestas*, Lid Editorial, Madrid, 2014, p. 33. They propose a new term for national security, which is more accurate, understanding as such an "ideal situation arising thanks to the effective and joint action of the State and other actors where the freedom and welfare of its citizens, the defence and integrity of its territory and its constitutional principles and values, together with international security, would be fully guaranteed and protected". Similarly, but with an approach based on risks and threats, FERNÁNDEZ HERNÁNDEZ, A. "Ciberamenazas a la Seguridad Nacional", in González Cussac, J.L. & Cuerda Arnau, M.L. (Dirs.), *Nuevas amenazas a la Seguridad Nacional*, Tirant lo Blanch, Valencia, 2013, p. 163, as he considers that within the term NS should be included all risks that threaten state integrity and the survival of the state political system, regardless of the nature of those risks. The latter can become threats which, in turn, can create damages that may endanger the survival of the State as such and all that it represents. For his part, FERNÁNDEZ RODRÍGUEZ understands that this concept has evolved to more all-encompassing and synergistic forms, and must be given an integral meaning, although it does not reach the dimensions of human security. FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es) en un futuro incierto (un estudio jurídico constitucional)*, Aranzadi, Navarra, 2020, p. 47.

[116] GOVERNMENT OF SPAIN, *Estrategia de Seguridad Nacional 2021*, Catálogo de publicaciones de la Administración General del Estado, Madrid, 2021, p. 54.

[117] GODOY, O. *Libertad y Seguridad en un contexto global. Retos y desafíos para los sistemas de garantía de los Derechos fundamentales*, Dykinson, Madrid, 2020, p. 19; CIAMPI, M. "Is 'security state' come paradigma della statualità contemporanea", in Forgione, A., Massucci, R. & Ferrigni, N. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milano, 2020, p. 100. Likewise, on the concern and threat to security posed by terrorist fighters returning to the West, see, CANO PAÑOS, M.A. "La amenaza proveniente de los combatientes yihadistas retornados a España. ¿Motivo de preocupación", *Revista de Estudios de Seguridad Internacional*¸ vol. 8, nº. 2, 2022, pp. 189 and next.

terrorism, mainly carried out by Islamic fundamentalist groups, has different characteristics from those forms of terrorism that we could call conventional (e.g., ETA or the IRA). As the attacks cross state boundaries, the consequences are catastrophic. Moreover, one of the main objectives of these groups is to create a feeling of fear, anxiety and generalized insecurity among the public, since their unpredictable actions are usually directed at everyday areas of community life. For all these reasons, a transnational response has been deemed necessary with the adoption of effective preventive measures to contain terrorism[118].

The fight against it has taken centre stage in EU policies and has become a key point in the common political strategy, both in security and defence. As a result, States are increasingly tending to implement mechanisms to limit citizens' rights in order to maintain security and meet the growing social demand for greater preventive capacity from public authorities[119].

Given that current threats go beyond the limits of the state and affect the community, we speak of a global risk society[120], characterized by the emergence of new and complex crimes, an increase in fear or a feeling of insecurity among citizens[121] and the emergence of the dogma of prevention. It also brings with it a change in the field of criminal policy from traditional criminal law to the model of preventive security[122] . This risk society is based on three fundamental pillars:

1) Threats cannot be delimited temporally and geographically, since risks are changeable;

[118] The difference between traditional and current forms of terrorism has required an adaptation of the instruments used by democratic societies, both to prevent attacks and to prosecute terrorists. Following the attacks of September 11, 2001 and other incidents in Europe in the aftermath, states have tightened their security policies; MYTHEN, G. & WALKLATE, S. "Terrorism, Risk and International Security: The Perils of Asking: 'What if?'", *Sage Publications. Security Dialogue*, vol. 39, nº. 2-3, 2008, p. 223. The authors criticize the Western countries' treatment of the new terrorist threat. They refer to the discourse of (in)security and the development of a culture of fear based on the terrorist phenomenon to influence political decisions.

[119] GODOY, O. *Libertad y Seguridad en un contexto global...*, cit., p. 19. The author goes on to point out that the need for the adoption of these measures is not disputed, but she does emphasize that they must respect fundamental rights. Similarly, SORIANO MORENO, S. "Las reformas legislativas en los Estados miembros de la Unión Europea frente al terrorismo: análisis desde los derechos fundamentales", in Godoy, O. (Coord.), *Libertad y Seguridad en un contexto global. Retos y desafíos para los sistemas de garantía de los derechos fundamentales*, Dykinson, Madrid, 2020, p. 81.

[120] FERRIGNI, N. "La sicurezza come metodo, il metodo nella sicurezza", in Forgione, A., Massucci, R. & Ferrigni, N. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milan, 2020, pp. 41-42. In modern society, risk assumes a global dimension for which the global consequences and dangers, the fruit of our society's decisions, contrast with the language of control used.

[121] Insecurity leads to dependence on increased protection. Along with terrorism, CIAMPI adds diffuse urban crime, social unrest in the suburbs, environmental and health risks, as well as the massive arrival of illegal immigrants and the breakdown of the rules of coexistence. Fear of such issues has the direct effect of spreading a feeling of precariousness and apprehension for the future, heightened by the media. CIAMPI, M. "Is 'security state' as paradigma della statualità contemporanea...", cit. p. 94.

[122] SIEBER, U. "The paradigm shift in the global risk society: from criminal law to global security law - an analysis of the changing limits of crime control", *Journal of Eastern European Criminal Law*, nº. 1, 2016, p. 16.

2) Increased potential for damage, among other issues, due to the acceleration of techno-scientific development;
3) Existing security methods cannot cope with the destructive force of the new risks[123].

As can be seen from the above, risk and security are intimately linked. For this reason, together with the former risk society, we also refer to the "security society", the two being a mirror image of each other. The latter is a society in which greater awareness of risks generates new demands for security. In this society, moreover, the fear caused by the presage of possible future damage translates into the search for a condition of security in the present, to which institutions respond by adopting measures aimed at maintaining it in the so-called "high social risk contexts"[124], among which terrorism can be included.

The fact that it is based on unpredictable attacks makes it difficult to estimate risk. Thus, what was once material and predictable has become intangible and unpredictable, since the risk was previously identified with a known enemy acting against an established order. Today, however, that enemy is unknown, making it difficult to maintain security[125]. A central strategy for containing the threat posed by risk includes intelligence and data that can inform threat assessments and make predictions of potential wrongdoing. This has brought about a significant change in the regulation of this phenomenon, directed at the future with a prevention approach[126], based on the development of security policies to address emerging risks.

In this new risk society, not only terrorism is of concern, but also other serious forms of crime such as organized crime[127] or cybercrime[128]. Added to all this are the changes in subjective and objective levels of welfare, which have led to greater terror of crime and an increased sense of insecurity, leading to calls for the adoption of stricter laws[129]. Thus, a new paradigm of social control based on security arises, in which

[123] MYTHEN, G. & WALKLATE, S. "Terrorism, Risk and International Security...", cit., pp. 223-224.

[124] FERRIGNI, N. "La sicurezza come metodo...", cit., pp. 45 and 46.

[125] EMANUELE, M. & FERRANTINO, T. "Rischio e complessità", in Forgione, A., Massucci, R. & Ferrigni, N. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milan, 2020, pp. 184-186.

[126] MYTHEN, G. & WALKLATE, S. "Terrorism, Risk and International Security...", cit., pp. 233-234.

[127] See, more extensively, SANSÓ-RUPERT, D. & GIMÉNEZ-SALINAS FRAMIS, A. "Crimen organizado", in De la Corte Ibáñez, L. & Blanco Navarro, J.M. (Dirs.), *Seguridad Nacional, Amenazas y Respuestas*, Lid Editorial, Madrid, 2014, pp. 133-148. The authors, on p. 145, state that some initiatives launched against this type of crime are aimed at the implementation of new criminal procedural and police investigation techniques, which must be combined with respect for human rights and the guarantees of the rule of law.

[128] While it is true that terrorism is the most striking of the risks and threats to security because public opinion is particularly sensitive to it and is affected by the fear that terrorist acts seek to generate, and because it has become more widespread in recent years. FERNÁNDEZ RODRÍGUEZ, J.J. "How to respond to security challenges? Una aproximación desde la dogmática de los derechos fundamentales", in Godoy, O. (Coord.), *Libertad y Seguridad en un contexto global. Retos y desafíos para los sistemas de garantía de los derechos fundamentales*, Dykinson, Madrid, 2020, p. 30.

[129] Insecurity, fear and the perception of fear are interconnected issues that have seen security progressively drift towards a totalizing horizon. Fear, filtered by sensory distortions of reality, generates insecurity. Thus, perception can be altered by fear or, on the contrary, be the triggering cause of fear,

preventive criminal law is combined with other legal systems also aimed at prevention[130], such as administrative law, police, intelligence, war and civil law. In combination with all of the above, we speak of a "security law", understood as the "norms dealing with the prevention of risks caused by human activities"[131].

As can be seen from the above, criminal law is losing its monopoly in the field of crime control, mutating into a preventive tool. The problem with this new orientation is that civil liberties are put at risk. SIEBER puts forward three reasons when making this assertion:

1) The new threats and fear of crime are causing a climate that prioritizes the objective of security, where the protection of rights comes second, especially privacy;
2) Prevention, risk reduction and safety are borderless concepts in principle. Whereas traditional criminal law was directed towards the repression of a previously committed crime, i.e. towards a specific event fixed in the past, prevention depends on an open and future-oriented prognosis. Absolute security is impossible to achieve, so it will always be necessary to go further in order to guarantee it, often at the expense of citizens' rights;
3) There are discrepancies between the different disciplines in charge of security law with a view to legal safeguards, since the goals and tasks of the different systems used for crime prevention are very different[132].

From all that has been explained in this section, it can be concluded that today's society is facing new risks and threats caused by new forms of serious crime, which seriously endanger the social order, giving rise to feelings of fear and insecurity among citizens. On many occasions, these feelings are encouraged by the way they are treated by the media or by the governments themselves, which take advantage of such situations

provoking the circuit of insecurity, whether real or perceived. CASTALDO, M.E. & NADDEO, M. "Sicurezza e controllo prevenzionale. Le misure di prevenzione tra passato e futuro", in Forgione, A., Massucci, R. & Ferrigni, N. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milan, 2020, p. 104.

[130] The approach to prevention is not a new issue, since in the 1990s, after the fall of the "Iron Curtain", new preventive security concepts emerged, such as "internal security", defined by the objectives of guaranteeing the welfare and stability of a society in the face of any endogenous threat, thus overcoming the idea of "public order". In Spain, during the period of democratic transition, the term "citizen security" was introduced, linked to the protection of persons and property against violent actions or aggressions, situations of danger or public calamities. For its part, in 1994, the United Nations Development Program established the concept of "human security", which emphasizes the guarantee of social rights as a basic and higher priority of state interests, and is more related to the promotion of development policies than to the use of military and police tools. See, more broadly, JAIME, O. et al. "Aproximación a la Seguridad Nacional...", cit., pp. 18-19. Similarly, FERNÁNDEZ RODRÍGUEZ, J.J. "¿Cómo responder a los desafíos de seguridad...", cit., p. 31, argues that the current concept of security has evolved towards that of human and natural security, going beyond that of citizen or national security, since it is not limited to an internal and an external vision, being "polyhedral" and "heterogeneous".

[131] SIEBER, U. "The paradigm shift in the global risk society...", cit., p. 26. The author indicates that these activities can be specified as acts that are or should be covered by criminal law and points out that such a limited approach concentrates on the most serious acts and their respective methods of control. He goes on to point out that the term should be limited in its definition to law aimed at eliminating risks, dangers and damages.

[132] *Ibd*., pp. 26-27.

for their own benefit in order to obtain some kind of political gain. For this reason, the adoption of more preventive measures is demanded, regardless of the possible collision that they may entail for rights and freedoms. This has led to a social model based on the prevention of the risk of crime, based on the implementation of actions aimed at eliminating any subjective threat of crime and, thus, the feeling of insecurity.

III. INITIAL INTRODUCTION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN CRIMINAL MATTERS

As we have had occasion to observe, crime continues to be a serious threat to public safety. The new manifestations of crime pose high risks to public safety at all levels, both at the supranational level and within state borders and at the local level, generating a sense of alarm in society. To combat this supposed lack of security, measures are being taken to prevent criminal activity, including ICT and AI-based systems. These tools are very useful in the police field, as they allow agents to carry out their work more quickly and effectively, including crime prevention[133]. However, technological advances not only favour police work, but can also be used as a means of committing crimes[134], both traditional crimes committed using such tools and new crimes committed through them[135]. Not only that, but these systems can also be subject to attack, thus creating new risks.

The impact of AI on crime is reflected in the increase in criminal opportunities. Crime in the new era posed by AI has shown novel dynamics, producing a change in the structure of crime. Following the criminological approach of opportunity established by FELSON and CLARKE[136], specifically the routine activity theory, we understand that crime occurs if a motivated offender, a suitable target and the absence of effective

[133] Technology plays an important role in policing and technological innovation has evolved along with police practice. LAUFS, J. & BORRION, H. "Technologicacl innovation in policing crime prevention...", cit., p. 190; ORTEGA ANDEREZ, D. et al. "The rise of technology in crime prevention: opportunities, challenges and practitioners' perspectives", *arXiv preprint: 2102.04204*, 2021, p. 2. The latter point out that the use of ICT is crucial for understanding and responding to crime problems. However, compared to the industrial field, they argue that their introduction has been more limited in terms of crime reduction. On pp. 8-14 they present various ICTs that have proven useful in crime prevention, including some that use AIs such as edge computing.

[134] NINAQUISPE SOTO, M.E. et al. "Technology and crime prevention: A systematic review of literature", *2021 Fifth World Conference on Smat Trends in Systems Security and Sustainabiligy (WorldS4)*, IEEE, 2021, p. 275.

[135] In this regard, it should be noted that cybercrime is no stranger to the advances and advantages offered by AI for greater success in the commission of crime, as it allows criminals to target their resources more effectively, thus achieving greater impunity. This makes personal identification and attribution of responsibility more difficult. RIESGO GARCÍA, M. "Inteligencia Artificial. Enfoque policial", in Peralta, Salvador Torres and Herrera (Coords.), *El Derecho y la Inteligencia Artificial*, Editorial Universidad de Granada, Granada, 2022, p. 483.

[136] Within this approach, the authors include three different theories that analyze the way in which physical spaces produce crime. All of them are based on the principle that easy or tempting opportunities attract people to commit crime. Thus, they conclude by assuming that opportunity is a cause of crime. FELSON, M. & CLARKE, R.V. "Opportunity Makes the Thief. Practical theory for crime prevention", *Police Research Series, paper, 98*, 1998, pp. 2-3.

guardian[137] converge spatiotemporally. According to the principles of criminal opportunities set out by the authors cited above, social and technological changes favour the emergence of new opportunities[138]. In this sense, AIs have represented an unprecedented advance in global technological evolution, as they can carry out tasks similar to those performed by humans, sometimes even surpassing them, as shown above in the first section of this Chapter. More specifically, FRs appear as a strategy for situational crime prevention and reduction of criminal opportunities from the moment they imply an increase in surveillance in a given area or can be used *a posteriori*, through the analysis of video recordings derived from such mechanisms. This technique can lead to a decrease in criminal opportunities and an increase in the perceived risk of offenders if they know that the police can use such systems[139].

In our opinion, the superior advantage of the use of AIs in criminal matters compared to previous mechanisms is the reduction of time and space they entail. In this sense, if a mechanism is trained for the specific purpose of committing a crime, it entails little, if any, additional effort and cost to the person who designed it to execute the offenses, in addition to occurring in a more limited time span. Some of the most frequent crimes committed using AIs are scams, identity theft, pornography, software that attacks Internet security, viruses, etc.

Given the challenges and threats that all this entails, the following will address the question of how AI is used as a tool for the commission of different types of crime and can also be the object of attack. On the other hand, the issue of crime prevention using these tools will be discussed. This serves as a general introduction with which it is intended to lay the foundations of the way in which such systems are being implemented in criminal matters. This brings together the two sides of the same coin of crime, namely, its commission and prevention. The application of RBIS, especially FR by police to protect citizens from crime, will then be studied in greater depth, along with other purposes such as the discovery of the whereabouts of missing persons.

1. AI and its relation with criminal commission

Technological advances and innovations extend to all social activities. Crime, unsurprisingly, is also influenced, as criminal individuals use such systems as a tool to commit crimes, whether traditional or novel ones specific to this environment. AIs are

[137] *Ibd.*, p. 4.
[138] *Ibd.*, pp. 22-23.
[139] PIZA, E.L. et al. "CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis," *Criminology and Public Policy*, vol. 18, nº. 1, 2019, p. 137. The authors study CCTVs as a crime prevention tool by applying situational prevention theory. Thus, they consider that they are a mechanism that impacts the choice of offenders by persuading them to refrain from crime. In our opinion, what has been established for the former could also be extended to the facial recognition mechanisms inserted in such systems.

expected to play a key role in criminal acts in the future[140]. Organized crime is one of the areas in which they have begun to be used, those being determinant for their success. The fact that criminal organizations are equipped with modern technological systems has severe consequences, because the repercussions of the actions of criminal organizations in terms of danger, intensity of damage and number of victims often exceed the state's capacity for containment, constituting a threat to the security of society and an attack on state sovereignty and the democratic constitutional order[141]. In the specific case of AIs, there is concern about the processing and data management capacity involved[142]. The new ways of transferring information entail the transformation of the nature of security threats, so that they can access useful information not only to obtain competitive advantages in order to improve and expand their businesses, but also to articulate self-protection measures aimed at evading state punitive action.

The implementation of the AI mechanism itself entails various criminal threats. One of them refers to the danger posed by the possibility that the system may act in a more sophisticated way, exceeding initial expectations or possibly acting autonomously. The new behaviour could have unlawful implications, insofar as it departs from the original design and may lead to actions that, for example, may be an intolerable infringement of citizens' rights and freedoms. Non-predictability and autonomy may confer a greater degree of responsibility on the machine, but it also makes it more difficult to trust it. The main problem in this regard relates to the fact that the mechanism may undermine existing accountability models, threatening the deterrent and restorative power of the Law. It is difficult to determine the legal response to be adopted when an AI is the author of a criminal act. It may be that the mechanism acts completely autonomously or that it is under human control. In the latter case, there would be no doubt about the possible criminal liability arising from the offense, since it would fall on the person in charge of the system, while in the former case it could generate, if not a certain vacuum of liability, a complicated legal treatment[143]. The fact that the machine can perform a criminal act leads to the possible inadequacy of existing liability models to address the future role of AI in criminal activities. Therefore, the limits of liability models may undermine the certainty of the law, as artificial agents may commit crimes without meeting the conditions of liability for a particular crime.

Different crimes can be perpetrated through the AI, among which are the highest rate of successful cyberattacks; discovery of passwords for Wi-Fi theft or illegitimate access to certain places, whether physical or virtual, bypassing CAPTCHA control

[140] Despite this, KING et al. argue that the importance of AIs in criminal matters is not well known at present. The existing literature on their ethical and legal implications focuses on their regulation and control in civilian uses, rather than considering their possible involvement in crime. KING, T.C. et al. "Artificial Intelligence Crime...", cit., p. 90.

[141] SANSÓ-RUBERT PASCUAL, D. "Inteligencia artificial al servicio de la criminalidad organizada ¿Mito o realidad?", *Revista Ábaco*, vol. 1, nº. 103, 2020, p. 129.

[142] *Ibd.*, pp. 130-131.

[143] DE LA MATA BARRANCO, N.J. "Inteligencia artificial autónoma y responsabilidad penal de las personas jurídicas," *Almacén de Derecho*. Electronic resource obtained through the Web: https://almacendederecho.org/inteligencia-artificial-autonoma-y-responsabilidad-penal-de-las-personas-juridicas, [retrieved on January 26, 2024].

systems, deepfakes, etc.; calls simulating the voice of a real person (robocalling); cyberattacks on AI with intrusion and manipulation objectives, being very worrying the attacks on banks; fakenews and manipulation of autonomous cars[144].

In the trading domain, AIs can be used in financial markets and insolvency through price fixing and collusion, insider trading and market manipulation. Models based on the latter that feature artificial trading agents have shown that through reinforcement learning, an AIs can learn –among others– the order book spoofing technique. This involves giving orders with no intention of subsequently executing them and thus manipulating honest market participants. In the case of collusion, automated systems have planning capabilities and autonomy. Virtually instantaneous price information serves a coordinating function. When agents develop price-altering algorithms, any price drop by one agent can be immediately matched by another. Although this is not detrimental and represents an efficient market, when the possibility of a price reduction being responded to in kind, it disincentives the market and thus fulfils the punishment condition. At the same time, the ability of systems to learn and refine their capabilities means that they can develop new strategies, which makes it difficult to detect their fraudulent actions[145].

With regard to harmful or dangerous drugs: trafficking, purchase, sale and possession of prohibited substances, AIs can act as a tool to support trafficking and sale. Thus, for example, offenders can use unmanned vehicles that rely on AI planning and automation as tools to improve smuggling success rates[146].

In the area of crimes against the person, it should be noted that the most frequent crimes committed with AI are harassment and torture. Currently, more sophisticated fake content can be created with AI, so it is possible that new forms of harassment may occur. An example could be deepfakes or multimedia content manipulated with DL algorithms[147], especially videos and images that use the face of a real person but are artificially created by a machine that recreates even the person's body with great precision, usually with sexual or pornographic content. Celebrities are frequent targets of this type of situation. A case that generated alarm is that of singer Taylor Swift in January 2024. Pornographic videos with the singer's face were posted on the social network X (formerly Twitter). The images took more than a day to be deleted and reached 47 million views. It was the fans themselves who alerted of the situation and encouraged the removal of the aforementioned content[148]. However, it does not only affect celebrities, as anyone can be subject to this practice. In Spain, in the summer of 2023, images of more than twenty

[144] RIESGO GARCÍA, M. " Inteligencia Artificial. Enfoque policial...", cit., pp. 486-487.

[145] KING, T.C. et al. "Artificial Intelligence Crime...", cit., pp. 97-100.

[146] *Ibd.*, pp. 100-101.

[147] Not only is the technique used to create videos, but also images and voice recordings. CROSS, C. "Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging", *Crime Prevention and Community Safety*, vol. 23, 2022, p. 34.

[148] SANER, E. "Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in box'", *The Guardian*, 31 January 2024. Electronic resource obtained via the World Wide Web: https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box, [retrieved on February 7, 2024].

naked girls and young women between 11 and 17 years old, created by AI, were published and disseminated on social media. This content was developed from photographs of the minors taken from their own profiles and subsequently processed using an application that creates an imagined visualization of what the person would look like without clothes. Eleven young people between the ages of twelve and fourteen were apparently involved, either in the creation of the images or in their circulation through apps such as WhatsApp and Telegram[149]. This can cause psychological and emotional harm to the people involved, damage their reputation and credibility[150]. Due to the high precision they achieve, it is very difficult for people to discover that the content corresponds to a deepfake. For this reason, systems have been developed to detect it. The most widespread is convolutional neural networks (CNN), whose effectiveness is based on their ability to extract specific features from images and videos, distinguishing the details that manifest the forgery. The technology uses ML with a large data set, through which anomalies and inconsistencies in the composition of the manipulated material are identified[151].

On torture, the risk of AIs appears when developers integrate the mechanism into an interrogation. This is the case of automated deception detection in a prototype robotic guard for U.S. border control. The use of AIs in this field is motivated by their alleged ability to better identify deception, emulation and affect modelling to manipulate the interrogated. An AI with such capabilities can learn to torture a victim, applying psychological or physical torture techniques[152].

Theft and fraud; forgery and impersonation: the literature reviewed connects forgery and impersonation through AI with non-corporate theft and fraud, and also involves the use of ML in fraudulent enterprises. On non-corporate theft and fraud, a two-stage process is described that starts by using AI to obtain personal data and use it later, as well as other types of intelligent systems to create an identity that convinces the user to perform a transaction[153]. Another peculiar form of fraud is also linked to the aforementioned deepfakes and is catfish, based on the creation of fake profiles on dating platforms and social networks to seduce another person and obtain a financial gain from them through deception. The evolution of AI and ML in this field have the potential to increase the ability of criminals to perpetrate this crime[154], which can be executed either by stealing images of other users or by creating synthetic images accompanied by

[149] HEDGECOE, G. "Outrage in small Spanish town over AI-generated images of dozens of naked girls and young women," *BBC News*, 25 September 2023. Electronic resource obtained via the World Wide Web: https://www.bbc.com/mundo/articles/cz9r6792k13o, [retrieved on February 7, 2024].

[150] GUTIERREZ SULLCA, E.M. "Artificial intelligence techniques for detecting deepfakes and their impact on the veracity of online content", *International Journal of Systems Engineering*, vol. 4, nº. 2, 2023, p. 8.

[151] *Ibd.*, p. 7.

[152] KING, T.C. et al. "Artificial Intelligence Crime...", cit., pp. 101-103.

[153] *Ibd*., pp. 104-106. pp. 107 and next. They set out a series of possible measures. If the legislation does not prohibit high levels of autonomy for the mechanisms, the regulations have to force freedom to be managed with technological remedies to prevent emergent criminal acts or omissions.

[154] CROSS, C. "Using artificial intelligence (AI) and deepfakes to deceive victims...", cit. p. 31.

different materials that are not of a real person. To combat this practice, tools are being developed to detect such images[155].

AI, as we indicated above, can not only be the executor of crimes but also the target of them. Systems can be attacked in different ways and for different purposes. An AI that has not been developed with a cybersecurity mechanism from the beginning may be vulnerable to cyber-attacks that target the AI data, model or algorithm and lead to undesired results or wrong decisions[156]. The case of WikiLeaks, a leaks site created by Julian Assange, is quite significant, as it led to the massive leak of confidential U.S. documents. First the "Afghanistan Diaries" were published, then the "Iraq War Logs" and "Cablegate"[157]. All this had a great impact because major political and financial scandals were brought to light.

There are several ways in which systems can be attacked, both in the training phase and once they are up and running. They are listed below. Firstly, the "data access" attack, as its name suggests, consists of accessing the training information and using it to create a substitute model. In the "poisoning" attack, either the data or the model is altered, either directly or indirectly; for the former, various techniques can be executed such as data injection, data manipulation in the form of output labels or input, as well as logic corruption. In "evasion" attacks, the attacker solves a constrained optimization problem to find a perturbation in the input that results in the desired misclassification. Finally, in "Oracle" attacks, an individual uses an interface or API of the model to present inputs to the model, observe its outputs and thus obtain the desired information. The tactics used in the latter case are: (a) extraction, whereby the model's parameters or structure are obtained through observations on the predictions, including the probabilities returned for each class; (b) inversion, from which the inferred features can allow the attacker to reconstruct the data used to train the model, including personal information that violates an individual's privacy; and c) membership inference, in which the results returned by queries made to the model are used to determine whether particular data points belong to the same distribution as the training dataset and to exploit differences in the confidence given by the model about points that were or were not seen during training[158].

One solution to address the threats posed by the increasing use of AI for crime and the attack on it for illicit purposes is the use of AI. For this reason, AIs are not only used for criminal purposes, but also in the field of crime prevention, as will be discussed in the following section.

---

[155] *Ibd.*, p. 38.

[156] AYERBE, A. "La ciberseguridad y su relación con la inteligencia artificial", *Real Instituto Elcano*, nº. 128, 2020, p. 4.

[157] MIRANDA, B. "Julian Assange: here's what was the big leak of classified documents in 2010 for which the U.S. is seeking the extradition of the WikiLeaks founder," *BBC News*, 12 April 2019. Electronic resource obtained via the World Wide Web: https://www.bbc.com/mundo/noticias-internacional-47902652, [retrieved on 8 February 2024].

[158] AYERBE, A. "La ciberseguridad y su relación con la inteligencia artificial...," cit., p. 6.

2. AI as a tool for preventing and fighting crime

Technological advances have reached city infrastructure, to such an extent that we are now talking about smart cities[159]. Their main objectives are to guarantee the quality of life of citizens, better management of issues affecting the urban population and sustainability in every aspect of life. One of the main challenges of this new city model is precisely to guarantee public safety[160]. So these cities are connected with cameras and sensors that have embedded software that automatically collects data such as license plate numbers, behavioural pattern detectors and other systems such as facial recognition[161]. Likewise, the use of technology in crime prevention is becoming increasingly common and can contribute to crime reduction, with AI and ICTs[162] standing out among these new technologies, with which crime can be prevented before it takes place[163], making it possible to achieve greater citizen security.

In such a context, an area where prediction derived from AIs can improve the current state of efficiency, is policing[164], fighting against criminal commission and threats

[159] It is not our task to study smart cities in depth, as this issue is far beyond the scope of our study. However, we reproduce the definition offered by LAUFS/BORRION, who understand as such "any city that uses new information and communication technologies to improve the well-being of its citizens and make services more resource-efficient". LAUFS, J. & BORRION, H. "Technological innovation in policing and crime prevention...", cit., p. 191. The authors go on to point out that the "smartification" of city infrastructure and the rapid development of new technologies mean that professionals are faced with new solutions and new problems.

[160] BUTT, U.M. et al. "Spatio-Temporal Crime Predictions by Leveraging Artificial Intelligence for Citizens Security in Smart Cities," *IEEE Access*, vol. 9, 2021, pp. 47516-47517. The authors further argue that the significant increase in urban population poses significant challenges, including resource planning, public safety, and a large amount of data generated from sensors, cameras, and tracking devices. On the issues related to the risks posed by the Internet of Things (IoT) which includes, among others, the facial recognition system in the security of smart cities, see extensively, NERONI REZENDE, I. *Surveillance Risks in IoT applied to Smart cities...*, cit., pp. 7 and next.

[161] MOBILIO, G. "Your face is not new to me- Regulating the surveillance power of facial recognition technologies", *Internet Policy Review. Journal on Internet Regulation*, vol. 12, no. 1, 2022, p. 2.

[162] NINAQUISPE SOTO, M.E. et al. "Technology and crime prevention...", cit., pp. 257-283. The authors reached this conclusion after a systematic review of the literature on the use of technology in crime prevention. They identified eight technological tools as the most commonly used, the most frequent being those mentioned in the main text. See also CHANGO, X. et al. "Technology in forensic sciences: Innovation and precision", *Technologies*, vol. 12, nº. 120, 2024, pp. 1-25. The latter also include, among others, biometrics.

[163] MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal: Más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, nº. 20, 2018, pp. 98-110.

[164] Equally linked to crime is the judicial environment to support legal operators in making decisions on, among other issues, pre-trial detention or parole. This may collide with some fundamental rights, especially in relation to the guarantee of a fair trial. As a significant example in Spain, the Integral Monitoring System in cases of Gender Violence (*VioGén*), of the Secretary of State for Security of the Ministry of the Interior, which determines the level of risk of a victim of gender violence in order to establish the protection measures to be imposed. According to the Ethics Foundation Audit, the system has some shortcomings: it is not transparent, it has not been independently evaluated or audited, it is not accountable, it does not involve the end users who have never been consulted about the system in any of its phases. Added to this are new questions about the transition of the mechanism to ML, especially about the absence of public and open debate on this process. FUNDACIÓN ÉTICAS, *External Audit of the VioGén System*, 2022. Electronic resource obtained through the Web: https://eticasfoundation.org/wp-

affecting the state using a more effective management of resources[165]. The vast amount of information available to LEAs has increased in recent times due to the use of the Internet and digital tools. Information gathering is a central function of police forces and a fundamental resource for developing efficient investigations. Thus, AIs are being used in the field of crime prevention and as an investigative assistant[166]. The vast amount of data on previous offenses allows law enforcement agencies to study them and extract patterns and trends from the different types of crime committed in a given area.

content/uploads/2022/04/ETICAS-_-Auditori%CC%81a-Externa-del-sistema-VioGe%CC%81n-_-20220308.docx.pdf, [retrieved on March 18, 2024], p. 34.

[165] AI tools use mathematical algorithms to select and allocate police resources for crime prevention. In the opinion of MIRÓ LLINARES, such mechanisms constitute a tool of great potential. They consist of the application of quantitative techniques to identify targets of police interest in order to reduce criminal risk through the prevention of future crimes or the resolution of past incidents. MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal...", cit., p. 100; VALLS PRIETO, J., *Inteligencia Artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 32. Similarly, BLOUNT, who points out that prevention as crime control is a way of managing risk based on the prioritization of previous acts rather than on results and coincides with an increase in the criminalization of incipient acts. So the categorization of factors is becoming broader and broader, leading to a greater amount of information to be managed, thereby increasing the need and desire for more efficient management through which the likelihood of crime can be identified and addressed. It is at this point that AI is considered that it can alleviate the burden of having to assess a wide network of factors. AIs extrapolate criminal correlations from a large number of data categories, allowing the construction of a profile by which individuals can be identified as potential crime suspects. These systems are able to accurately synthesize information to interpret relationships that may indicate a higher risk of future events through risk assessment. This is a police tool with which suspicions can be generated, because identified and evidence evaluated, thanks to its instant and systematic analysis of large and varied data sets. Thus, it directs officers to patrol areas that are considered to be at high risk of future crime based on the outcome of the crime assessment. The expectation that future crimes/offenders will be like those of the past, and that, for example, neighbourhoods that share similar factors could be prioritized as a probabilistic risk factor for crime. An example of a risk assessment system used for predictive policing is "ShotSpotter," which works by analyzing crime data by 250 square meter areas to determine where criminal offenses are most likely to occur. With this information, officers are dispatched to the identified areas and offer guidance on the types of crime that are most likely to occur as well as more effective intervention tactics. The program also keeps track of interactions between officers in these areas to ensure that they are not over-policed and determines the police patrols that would be most effective in containing crime. It does, however, prioritize policing in neighbourhoods or areas where crime is most likely to occur, which can lead to problems such as mistaken identifications. The most important types of data used by these technologies are previous crimes. The historical information from these informs the "profile" of particular crimes; from the opportunistic location, to the most advantageous time of day, to the characteristics of the likely perpetrator. The more information that can be accessed, the greater the degree of certainty that can be achieved in predicting when and where the next crime is most likely to occur. What is more controversial is that even profiles of individuals who might offend in the future can be created, and problems may arise in relation to the biases contained in the data with which the algorithm operates.
BLOUNT, K. "Using artificial intelligence to prevent crime: implications for due process and criminal justice", *AI & Society*, 2022, pp. 3 and 4. LED has pronounced on biases, specifying in its Nº. 8 that they can be inherent to the underlying data sets, especially when using historical data, introduced by the developers of the algorithms or generated when the systems are applied in real-world settings. So the results of AI applications depend on the quality of the data used. Such biases tend to gradually increase, perpetuating and amplifying existing discrimination, particularly of people belonging to certain ethnic groups or racialized communities. It continues in Nº. 9 by pointing out that AI predictions based on the characteristics of a specific group of individuals amplify and reproduce existing forms of discrimination. It therefore concludes by pointing out that great efforts must be made to avoid this.

[166] MATTA, W. "L'intelligenza artificiale per la sicurezza pubblica", in Massucci and ferrigni (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, Franco Angeli, Milano, 2020, pp. 283-284.

A number of tools have been developed for this purpose. For example, PredPol, which calculates predictions of future crime events to facilitate patrol management, especially in geographic areas with high crime rates. It uses historical event data sets to train the algorithm, and this information is then updated daily with the different crime situations as they arise[167]. This allows for more effective measures to be taken to combat such disruptive phenomena in the community. In this sense, identifying hotspots or areas where there is a higher concentration of crime, as well as forecasts of crime at a specific time and place will allow for better management of available police resources[168]. Thus, AIs are an important tool in this environment, as they enable the rapid analysis of information on past events, thus generating crime maps and patterns that allow, among other things, the identification of future crime trends in a physical or virtual environment, facilitating a more appropriate management of crime control and prevention instruments.

AIs are not only used for the aforementioned purpose, while other applications have been developed for the prediction of specific offenses. This is the case of the tool created by WANG and MA to detect crime in the field of public health, which involves a wide range of social factors and specific characteristics. For this reason, it is not possible to know and process all the information manually in an agile way. Thus, the support of the vector machine allows to extract elements from the data combined with the random forest algorithm to have a predictive model with more appropriate results[169] obtained in a faster and more agile way.

---

[167] *Predpol*. Electronic resource obtained via the World Wide Web: https://www.predpol.com/, [retrieved on December 19, 2023].

[168] BUTT, U.M. et al. "Spatio-Temporal Crime Predictions by Leveraging Artificial Intelligence for Citizens Security in Smart Cities...," cit. pp. 47520-47522. The authors further make a proposal for an algorithm to detect hotspots that can perform two tasks. On the one hand, to detect the regions with the highest crime density and, on the other hand, to predict the number of crimes in each region with high crime density. To perform them, the algorithm they propose is a combination of two different algorithms each to perform each of the above tasks. They analyzed three regions and obtained very positive results when compared with other predictive programs. One of them, that in areas of lower crime density the predictions are more effective.

Another study in which an algorithm is developed to predict the areas of the city with the highest risk of committing crime is the one carried out by WANG, et al. WANG, Q. et al. "CSAN: A neural network benchmark model for crime forecasting in spatio-temporal scale", *Knowledge-Based Systems*, nº. 189, 2020, pp. 1-5.

On the other hand, crime prediction is presented as a promising solution to address crime. The main objective of crime prediction is to efficiently and realistically predict crime patterns in order to provide relevant solutions on possible future crime trends based on the analysis of past crime data. One of the advantages of crime prediction is the prevention of crime manifestation in areas or regions based on previous patterns, thus providing ideas for allocating appropriate resources within the community, which facilitates better police coverage and useful information for authorities, thus efficient solutions in crime preventive measures can be planned. KHAIRUDDIN, A.R. et al. "A review on applied statistical and artificial intelligence techniques in crime forecasting," *IOP Conference Series: Materials Science and Engineering 551*, 2019, p. 1.

On criminal prediction and the risks it entails, see, ZAVRSNIK, A. "Criminal justice, artificial intelligence systems, and human rights", *ERA Forum*, vol. 20, 2020, pp. 567-583. The author also discusses the introduction of AIs in criminal justice in general, so it is of great interest to consult it to learn more about this issue that is generating so much debate and controversy, especially because of its impact on fundamental rights.

[169] For a more detailed account of the process of developing and creating the system, see more extensively, WANG, H. & MA, S. "Preventing crimes against public health with artificial intelligence and

The systems implemented in this sense, as mentioned above, have some advantages in the field of crime prevention and control, since they speed up police work and allow for a more efficient management of available resources. However, they may have some detrimental effects since, as D'ALOIA points out, the tools for crime prevention or for calculating recidivism may be based on information that ends up feeding a kind of vicious circle, whereby an individual's poverty or family conditions, place of residence, academic career or racial minorities will be criminalized[170].

Likewise, if we take into account what has been pointed out in this section together with the preceding one, we can affirm that AI is a "double-edged sword", since it has caused an increase in the crime rate[171] and a change in the dynamics and structures of crime; but, on the other hand, it offers technical support for the analysis and prediction of crime before and after it has been committed, in the latter case, collaborating with the judicial system in terms of procedural evidence[172].

machine learning capabilities", *Socio-Economic Planning Sciences*, no. 80, 2022, pp. 4-5. As an example, other predictive mechanisms are those created by PRIYANKA et al. who implemented an analysis system that not only predicts crimes using the initial information with which it was created, but also updates itself with data from new reports as they emerge. PRIYANKA, D. et al. "Incremental classifier in crime prediction using bi-objective Particle Swarm Optimization", *Information Sciences*, nº. 562, 2021, pp. 279 and next.

A similar tool was developed by ASIT, K.D. & PRIYANKA, D. "Graph based ensemble classification for crime report prediction", *Applied Soft Computing*, nº. 125, 2021, pp. 1-14; and that of KIM/JEONG, who conducted a study based on predictive AI to reduce the crime rate. To do so, they used open data of crimes committed in Baltimore City between 2011 and 2016 through multiclass logistic regulation. They tried to predict some crimes and the instruments with which they are committed by analyzing historical data recorded in the indicated period, with information regarding victims. For this, they used different variables, among others: the date of the crime, the time, the code that classifies the crime, where it occurred, the typology, whether the crime was inside or outside, tools used to commit it, area, neighbourhood, latitude and longitude and total number of incidents, etc. Likewise, to know the process by which it was developed and implemented, KIM, K.S. & JEONG, Y.H. "A Study on Crime Prediction to Reduce Crime Rate...", cit. pp. 17-20.

[170] Of this opinion, D'ALOIA, A. "Ripensare il Diritto nel tempo dell'Intelligenza Artificiale...", cit. p. 98.

[171] In this regard, some mechanisms such as the Strategic Subject List, which focuses on personal rather than geographic data and determines the likelihood of an individual being involved in a gun crime, have been scrutinized by RAND (a non-profit organization) and it has been observed that, instead of reducing crime rates by preventing the commission of crimes, they have increased the prison population. On the other hand, PredPol in the city of Kent in the United Kingdom included very minor offenses, which led to an increase in the detection of these offenses but did not work in those where the place or mode of execution was changed. VALLS PRIETO, J. *Inteligencia Artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 33.

[172] AI to support the work of the prosecution is mainly reflected in the automatic data analysis system for high-definition file data and sentencing suggestions. These can help the staff dealing with the case to efficiently process and accurately deal with the key information for a certain case. The result of applying AI in the criminal process is to improve the efficiency of the process, reduce litigation costs, and improve the level of court services, among others. WANG, H. & MA, S. "Preventing crimes against public health with artificial intelligence and machine learning capabilities", *Socio-Economic Planning Sciences*, no. 80, 2022, p. 4. An example of an AIs used in the field of criminal prosecution is the one designed by SILVA et al. The authors had the objective of speeding up the work of the prosecutor's office when evaluating all the existing data on a given case, sometimes in a very short time. This circumstance makes it difficult for the personnel in charge of investigating an incident to process all the information available about it and to be able to make appropriate decisions. They focus on digital criminal evidence, given that the increasingly widespread use of smartphones produces a large amount of data, which is difficult to analyze and process, especially when several can converge in the same case. Therefore, they proposed to

Given the duality of intelligent systems, their uses must be precisely regulated and limited in order to prevent them from expanding towards the execution of illicit purposes. On the other hand, it should be kept in mind that AIs are mathematical models that offer a probability of a crime taking place, based on prior information, which is why they cannot predict it with absolute certainty. For this reason, the results offered must be taken with caution. In addition, another controversial issue is the data sources used to train the algorithm, since the effectiveness of the tool will depend on the quality of the information contained in them. Thus, if it is only fed with information from, for example, disadvantaged neighbourhoods, it will only detect crimes committed in areas with similar characteristics, thus pursuing crime linked to poverty, which would lead to an increase in inequality and further stigmatize this sector of the population[173]. To avoid the above, the mechanism must be trained with data that is as varied and diverse as possible, as its effectiveness will depend on it.

Another concern arising from the use of AI and ML comes from the generation of new information based on the evaluation of existing data, by relations and correlations through combined categories which, in turn, can lead to the creation of more information through the continuous updating of algorithms, mimicking an intelligent being's ability to learn by inference. The main problem deriving from this situation is the possible lack of transparency of the process, also known as black box. Initially it is possible to identify the original algorithmic source code, all the data integrated in the system and the final result. However, in ML, as the system is updated with the new information it receives and generates, the source code is no longer up to date. In addition, if the original data is flawed, the result is affected. This can interfere with the agent's decision because human judgment is altered by the results of the algorithm. According to BLOUNT, the above causes a change in the relation between the citizenry and the police, because the officer's actions are no longer based solely on his own observations and knowledge, but on expectations. Thus, forming suspicions based on general profiles created by algorithms undermines the concept of individualized suspicion[174], on which any decision on the

use *a micro-services-based application* with AI with which large amounts of images contained in digital criminal evidence can be processed using open source software. This system identifies specific images of objects, such as firearms, ammunition, text documents, screenshots, etc., allowing an easier and faster processing of these, thus speeding up the criminal process. SILVA, I. et al. "Using micro-services and artificial intelligence to analyze images in criminal evidences", *Forensic Science International: Digital Investigation*, nº. 37, 2021, pp. 1-9.

[173] VALLS PRIETO, J. *Inteligencia Artificial, Derechos Humanos y bienes jurídicos...*, cit., p. 33.

[174] BLOUNT, K., "Using artificial intelligence to prevent crime...", cit., pp. 3-4. A profile is built on traits that are perceived as indicators of crime propensity among members of a group. It is a holistic picture that includes environmental factors, opportunities and generators of crime, as well as the role of the person who might commit crime and his or her characteristics. Predictive policing is seen as analogous to the "Stop and Frisk" program used by the New York City Police Department in the early 2000s. Officers did not stop people based on their individual suspicions, but by "categorical judgments" of those who fit a profile and by being in an area considered risky or if they exhibited evasive behaviour. This tends to disproportionately affect certain population groups. While certain areas may actually be more likely to experience certain crimes, it is only possible to know this to the extent that the offence is known and the others are proportionately categorized. In the program indicated, areas where more immigrants resided were categorized as having a higher risk of immigrants committing crimes compared to the general population. Because of the existence of more police in that area, community bias could occur resulting in more calls for assistance, or a higher likelihood that officers would be more likely to file a report in these cases. The

possible responsibility for the commission of a crime must be based. To detain a suspect, the officer has a standard of discretion, based on the information he has about the individual and act in question. However, the use of statistical tools such as AI is inherently outside the context of a given situation, since by their very nature they compare components of other past contexts and, therefore, is not an individualized decision[175]. This situation can lead to violations of the right to non-discrimination, given that, for example, if there is a police patrol in a high-risk area, it is not that it is more likely that a crime will be committed, but that it may happen that the officer observes individuals as potential suspects, which eliminates true objectivity and can lead to situations of discriminatory treatment.

Another right that is threatened by predictive policing tools is the presumption of innocence, which would be violated in many ways. One of them through an expressive and non-legitimate act of a police officer or authority suggesting the guilt of a subject. The presumption of guilt of an officer is nothing more than a descriptive and factual notion that applies situational awareness, while the presumption of innocence is a normative and legal fiction[176]. Whether or not both rights are violated depends on the proper application of policing standards, i.e., whether the formation of a suspicion is reasonable. Predictive policing necessarily alters the application of discretion and, as a result, the formulation of discretion, which in turn can undermine the application of individual rights directly and indirectly[177].

In the specific field of FRs, these are a tool that allows remote identification, even in a large crowd and in a short time, of criminals suspected of having committed a serious crime or terrorists for whom there is a search warrant, allowing, as we have said, their rapid identification and, if necessary, the initiation of criminal proceedings. They are therefore extremely useful in the law enforcement environment. In addition, they allow the identification of crime victims and missing persons.

However, and despite what has been mentioned so far, we are aware that AIs, if used correctly, with the knowledge of the users whose data are analysed, can improve the services provided by police officers. On the contrary, if they are used inappropriately, they can lead to an unacceptable intrusion in the aforementioned rights and freedoms of citizens, such as privacy, among others, and facilitate the use of personal data for harmful purposes that can, if necessary, endanger security, as well as lead to an Orwellian

end result is that people from these ethnic groups will more likely be targeted for preventive patrols. Automatically generated risk assessments are often no transparent about the content of their output and generally assumed to be an adequate prediction. Beyond the lack of individualization, these data are the result of police and community crime reports. This raises questions about the legal application of discretion and due process. Preventive profiles are indicators of actual conditions relevant to a potential crime, countering the concept of individualized suspicion. The profile is created on certain perceived traits.

[175] *Ibd.*, pp. 5-6.

[176] *Ibd.*, p. 7.

[177] *Ibd.*, p. 8. On p. 9 he further points out that most of the programs used for crime prevention, especially for risk assessment, are created by companies that do not necessarily have democratic policing objectives.

surveillance system[178] that can jeopardize security. The main objective of criminal law is to guarantee both the latter security and freedom, a difficult issue with the new trends in crime control and prevention since, as SIEBER states, we must deal with the necessary safeguards to avoid the abuses of crime control characteristic of the emerging security law[179].

Taking into account the considerations and limitations to ensure an appropriate use of AIs that combines the guarantee of citizens' rights and freedoms with the advancement of technology, society can benefit from the latter and favour the effectiveness of police action in the fight against crime.

Once some basic essential issues of AIs in crime prediction and prevention have been exposed in this section, in the following we will delve into the main subject of our work, which is the application of remote biometric identification systems in public places for law enforcement purposes by the agents who are entrusted with this task. Thus, throughout this research we will address the ethical and legal issues involved in the implementation of such mechanisms, especially the impact on rights and freedoms (Chapter III). On the other hand, Chapter IV will address the argument of the security benefits that tend to legitimize their use, while the following chapter, Chapter II, will deal with general aspects related to biometric identification techniques: how they work, how they have been used in the field of police investigation and the way in which they are regulated by the AIA.

[178] Of this opinion, DE LA CORTE IBÁÑEZ, L. & BLANCO, J.M. "Potenciadores del riesgo. Una visión ampliada para un mundo global", in De la Corte Ibáñez, L. & Blanco Navarro, J.M. (Dirs.), *Seguridad Nacional, Amenazas y Respuestas*, Lid Editorial, Madrid, 2014, pp. 74-75; & SIEBER, U. "The paradigm shift in the global risk society...", cit., p. 16.

[179] SIEBER, U. "The paradigm shift in the global risk society...", cit., p. 17.

CHAPTER II

APPROACH TO THE WAY OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS OPERATE AND THEIR REGULATION IN THE AI ACT

I. HOW BIOMETRIC IDENTIFICATION SYSTEMS WORK

1. Previous aspects

As an introduction to this Chapter, it is necessary to understand –at least briefly– how automated biometric identification mechanisms work. They are a pattern recognition mechanism that operates by acquiring biometric data from an individual, from which it extracts a series of characteristics that it then compares with the template established in the database[180]. The system determines the authenticity of a specific physiological or behavioural characteristic of the user[181]. This initial work will provide a better understanding of how they work when used in crime prevention and the ethical and legal implications of their use.

There is a wide variety of biometric recognition systems, ranging from the simplest ones aimed at very small groups of users, to more sophisticated ones capable of comparing a sample with the huge number of patterns stored and providing a result in a very short time. Despite the diversity of instruments, they all have common elements in their design, implementation and operation, which are described below.

In general, biometric procedures record a measurable biological characteristic with the capacity to individualize a person. Already at the time, in the corresponding section of this research, we explained what biometric techniques and data of this nature are, highlighting that they are a type of sensitive personal information, whose processing is currently carried out through automated procedures that include software and hardware, which use is restricted by European Community Law, as long as they are aimed at univocally identifying a subject. However, at this point, we wonder how such mechanisms are designed, implemented and operated, given that they are increasingly applied to more and more areas of society, including citizen security. Thus, at the EU level, some Member States use biometric characteristics in national identity cards, passports and residence permits. In addition, biometric data are being used on a large scale in certain sensitive issues such as asylum, immigration, automated border control and e-Government applications[182]. These are environments with specific characteristics, where citizenship rights are compromised, as is the case with residence or passage through a given country. For this reason, the use of biometric systems must be carried out with strict respect for the fundamental rights and freedoms that may be affected by their implementation.

[180] JAIN, A.K. et al. "An Introduction to Biometric Recognition...," cit., p. 4.

[181] PANKANTI, S. BOLLE, R.M. & JAIN, A. "Biometrisc: The Future of Identification...", cit. p. 46.

[182] REDING, V. "Foreword...", cit., p. V.

2. Digitalization of data

Humans have the ability to identify others through their physical or behavioural traits. What makes automatic biometric technology different from that performed by people through their own senses is the conversion from analogical to digital. We are therefore talking about a process of digitalization of identity, which is nothing more than a symbolic reduction of something in order to be able to work with it in a feasible way, which modifies the nature of the object represented, transforming the very nature of individuals into mere living objects that can be measured and compared with other similar ones. The effect of digitization is not only to reduce an object to a quantitative dimension, but to deal with the new dimension in a more rational way[183].

In such a way that, once one can operate with a number representing someone's encoded identity, a multitude of operations can be performed with it[184]. In line with the above, it is worth noting that the moment the representation of the qualities of an item is converted into digits, one operates with numbers. At this point, a person is no longer needed to evaluate the correspondence between a sample and its representation. On the contrary, we enter a new territory, the digital one, where recognition can be fully automatic[185], executed by systems specifically designed for this purpose.

3. Phases of the data collection and storage process

First of all, when developing any type of biometrics, a suitable sensor is needed to record the data related to the object to be measured. This is the first step in measuring what is to be identified[186]. When the sensor captures the data, it inevitably generates other types of information, such as information related to the time and location at which the detection occurred, so it is more than a passive recording[187] and is linked to other types of metadata.

[183] GHILARDI, G. & KELLER, F. "Epistemological Foundation of Biometrics...", cit., pp. 40-41.

[184] *Ibd.*, p. 41. For the authors cited above, the risk of working with a codified identity is to consider that the code really represents the original identity. The representation could be seen as a way of accessing the object, so that the identity of the object depends fundamentally on the representation adopted when analyzing it. On p. 43 of the same work, they point out that there are no quantitative data that can provide a real verification, but they offer a useful tool to proceed with an additional interpretation. For this reason, the latter is the real key to verification.

[185] MORDINI, E. et al. "Introduction...", cit., p. 7.

[186] GHILARDI, G. & KELLER, F. "Epistemological Foundation of Biometrics...", cit., pp. 30-31. Sensors would act in the same way as the senses of human beings. Sensors that measure first generation data are simple and capable of capturing and storing some physical characteristics of the recognized object. They can be optical scanners and do not act like the perception of a real individual, since, unlike the senses, the sensors do not work together. In the second generation there is an improvement in the perceptual domain, which is more similar to humans because it uses different types of sensors.

[187] *Ibd.*, p. 31.

Once the appropriate instrument is available, the process of obtaining and storing biometric data begins, divided into a series of phases that are grouped as follows: a) obtaining the information and preparing the standard, b) storing the standard, c) capturing the fresh standard, and d) comparing the latter with the other stored standards, with the consequent decision making.

The first, also called enrolment or obtaining biometric data from an individual's body[188], consists of the sensor scanning a person's physiognomy to create the digital representation. A feature extractor takes the so-called raw biometric data and processes it to generate a more compact and expressive representation[189] of the element being measured. This is translated into algorithms and proceeds to produce the template[190], which will be stored in a database[191] and used in identification or verification work. In this case, a new pattern of the individual is produced and compared with those already recorded[192]. After the capture of the sample, a pre-processing is carried out, with the aim of improving the image and facilitating the selection of the areas considered most optimal for obtaining the attributes that will be translated into algorithms or other mathematical representations susceptible to agile processing[193]. This phase is very prone to error because the systems depend on the veracity with which a person claims the identity that allows him/her to be included in the database, which does not depend on the recognition system used.

The storage phase is the one that raises the most problems or concerns. The digital supports in which they are inserted can be of several types: a) controlled by the source

[188] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., p. 179. A fundamental aspect of biometric-based systems is that they entail the availability of an individual's body, or some part of it, to be manipulated in certain ways, scanned and evaluated for particular purposes, as a prerequisite for the system to function. Bodies –or certain features of the body– are embedded in technical networks and play a role in a particular script. VAN DER PLOEG, I. "Security in the Danger Zone: Normative Issues of Next Generation Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 299.

[189] PANKANTI, S. BOLLE, R.M. & JAIN, A. "Biometrisc: The Future of Identification...", cit. p. 46.

[190] The template is the standardized representation of the biometric sample. It is necessary to obtain it because no physical property is immutable and can undergo changes throughout life. Therefore, if you want to get a reliable template to recognize a subject, it is necessary to merge signals captured at different times and conditions. GHILARDI, G. & KELLER, F. "Epistemological Foundation of Biometrics...", cit., p. 31. There are differences between the raw biometric data and the template that are important to take into account for judicial investigation purposes. Moreover, depending on how the information has been recorded, biometric data could be subject to different legal qualification and therefore different treatment, depending on whether they can lead to the identification of an individual, even if they can be understood as sensitive data. In this sense, see more extensively, GIROTTO, S. "Il trattamento dei dati biometrici", in Rodotà, S. & Zatti, P. (Dirs.), *Trattato di Biodiritto. Il governo del corpo, vol. I*, Giuffrè Editore, Milano, 2011, pp. 1240-1243.

[191] Such a database can be central or distributed, such as one in which each user's template is stored on a smart card carried by the individual. PANKANTI, S. BOLLE, R.M. & JAIN, A. "Biometrisc: The Future of Identification...", cit. p. 46.

[192] ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., p. 179.

[193] *Ibd.*, p. 180.

subject, i.e. the pattern is kept by the individual; b) database controlled by a third party but not communicated with the databases of other users; and c) networked storage. The choice of one system or another will depend on the technical organization and the purposes sought by the system in a given scenario[194].

Once the data has been stored, regardless of the medium in question, the recognition and issuing of the result can take place, thus reaching the last phase of the process. In this case, what happens is that when the individual is presented to the system, it takes a fresh sample that will be compared with those previously recorded. The mechanisms are "adjusted" to determine the level of tolerance allowed and the match is considered to be within a given confidence interval. This match can be of two types: "identification" when the comparison is with a database (or, in other words, one-to-many) or "verification" if it is with a specific template, i.e. a one-to-one comparison.

Strictly speaking, what is done is to teach the mechanism to search for similarities until it determines, after a comparison with all the stored patterns, whether there are matches between them and the real ones. If, as we say, the system confirms a match, the information associated with the biometric pattern in question can be accessed and this will allow the subject to be identified or his identity to be verified for the specific purposes for which its use is intended.

Thus, for the whole process described above to take place, biometric systems are designed with four modules: 1) sensor, which captures the biometric data of a subject; 2) feature extraction, in which the biometric data acquired in the previous module are processed to extract a set of salient or discriminatory elements; 3) matcher, in which the features extracted during recognition are compared with the stored templates to generate match scores. This module also includes a decision-making module, which confirms the identity claimed by the user or establishes an identity based on the score obtained; and 4) system database, used to store in a database the patterns of the users collected. The data recorded in the enrolment phase, depending on the system, may or may not be monitored by a person. Quality control is usually carried out to ensure that the sample can be properly processed in the subsequent phases. Depending on the application, the template will be stored in the central database of the biometric system or stored on a smart card held by the subject. Typically, several are recorded for the same person to account for possible variations in the biometric trait and the templates can be updated over time[195].

[194] *Ibd.*, pp. 181-183. If the system is a verification system and only needs to ensure that when a card or passport is used, the person carrying it is the person for whom it was issued, a chip can be used without the need for a larger database. When the system detects the presence of the passport, it searches the chip for the stored pattern and compares it with the freshly captured pattern. Thus, there is no off-chip storage.

[195] JAIN, A.K. et al. "An Introduction to Biometric Recognition...", cit. p. 6.

4. Distinction between verification and identification functions

Above, reference was made to the two purposes for which the system detects a person, i.e., identification and verification, which were also indicated in the first chapter. At this point, we consider it essential to specify, even succinctly, what each of them refers to, since this task is essential to understand the purpose of the RBIS under analysis.

In the case of identification, the aim is to conclude that the person under observation is –or is not– in the database. The templates of all users are searched to get the match. The comparison in this case is one-to-many to establish individual identity without the need for the subject to claim it. This way in which the mechanism operates is normally done for negative recognition purposes where it is intended to determine if the person is who he denies being, i.e. it seeks to achieve a negative identification in the sense of determining that an individual is not inserted in the database, as occurs in watchlists and, therefore, is not who the system intends to identify. In this case, the biometric sample is compared with the database to ensure that there are no matches. It is not of interest who is the individual under observation, but who is not[196]. Although this is the main task, it can also be used for positive identity verification for convenience because, while the latter can be done through traditional methods such as passwords, PINs, etc., negative identification is only possible through biometrics[197].

In the case of verification, the aim is to establish that the individual is the same person whose data is stored on the digital medium in question[198]. The main purpose in

[196] MORDINI, E. et al. "Introduction...", cit., p. 8. In the security field it is used, for example, to determine that a person is not among those who have previously applied for asylum in another country. An example of such a system is EURODAC in the EU, which involves the comparison of fingerprints of asylum seekers over the age of 14, as well as of persons apprehended for attempting to cross the Union's borders illegally or for fraudulently remaining on its territory. In addition to fingerprint information, other information such as the State of origin, sex, reference number of the State of origin, date of arrival, etc. is recorded. In this regard, see art. 11 of Regulation (EU) Nº. 603/2013 of the European Parliament and of the Council of 26 June 2013, on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) Nº. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) Nº. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast). The fingerprint of the subject in question is compared with all those stored in EURODAC, which indicates whether or not the subject is enrolled in EURODAC and, if so, the linked information. Another environment in which negative identification is very useful is the control of violent ultras in soccer matches, which are intended to prevent entry to stadiums to ensure compliance with the measures prohibiting access. On this last issue, specifically for the case of the facial recognition technique in matches classified as high risk, see extensively, DOMINGO JARAMILLO, C. "Aplicación del sistema de reconocimiento facial para prevenir la violencia asociada al deporte en los encuentros calificados de alto riesgo", in Calaza López, S. & Llorente Sánchez-Arjona, M. (Dirs.), *Inteligencia artificial legal y administración de justicia*, Aranzadi, Navarra, 2022, pp. 125-150.

[197] JAIN, A.K. et al. "An Introduction to Biometric Recognition...", cit., p. 5; PRABHAKAR, S. et al. "Biometric recognition: Security and privacy concerns", *IEEE Security and Privacy*, vol. 1, nº. 2, 2003, p. 34.

[198] MORDINI, E. et al. "Introduction...", cit., p. 8.

most cases is to allow access to physical or digital spaces to authorized persons[199]. The system validates the subject's identity by comparing the biometric data captured with the stored templates. That way when someone who wishes to be recognized claims an identity and the system performs a comparison to determine whether it is correct or not. Contrary to the previous one, this mechanism is normally used for positive recognition tasks, where the objective is to prevent several people from using the same identity[200]. This is the case, for example, of access control at airports.

Along these lines, in the USA, after the 9/11 attacks, "trusted passenger programs" were developed within the *RT program* of the STA (*Security Threat Assessment*), an agency of the *Department of Homeland Security*. The goal of the program is to pre-select passengers so that when they arrive at the airport they can pass through the controls more quickly than those who are not included in the same program[201]. The target population is smaller than in the previous case and is linked to U.S. citizens, nationals and permanent residents. Biographic and biometric data are collected and cross-checked with other databases of public and private institutions to ensure that only low-risk passengers are registered in the program. Once at the airport, passengers are matched and this allows them to pass through the airport more quickly. This mechanism has two complementary objectives. On the one hand, to speed up on-site security screening of passengers who have been screened and cleared by the STA and thus use resources more effectively. Biographical information is used to scan the applicant and decide whether or not to include him in the program. When accepted, you must submit your biometric data to the provider. Those are usually iris and fingerprints[202].

Once the way the system works has been explained, it is necessary to address the historical evolution of biometrics in general and of the FR in particular, from its beginnings to the current situation, in order to understand the different functions it has had, especially in terms of crime.

---

[199] The privacy risks of the verification function are more limited than in the case of identification, since it allows biometric characteristics to be stored locally, even under the absolute control of the individual. The control of personal data in these situations needs to be clarified, as does the determination of the applicable law. On the contrary, what happens in identification is that the data are not always under the strict control of the owner, so the privacy of the information may be at risk. SPROKKEREEF, A. & HERT, P. "Biometrics, Privacy and Agency", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 93.

[200] JAIN, A.K. et al. "An Introduction to Biometric Recognition...", cit. pp. 4-5.

[201] Similarly, the airline Vueling is implementing identity verification systems for its customers to speed up the boarding process by eliminating the need to show personal identification documents and boarding passes. To do so, it asks them to register their biometric face data in its application. In Spain, this system is also used by other airlines such as Iberia, Air Europa and Binter, and the registration in one of them allows the use of the system in the others. See, DÍAZ, M.P. "Vueling implanta el reconocimiento facial para embarcar en avión: así funciona y a quién se envían tus datos", *El Confidencial*, 19 January, 2024. Electronic resource obtained through the Web: https://www.elconfidencial.com/tecnologia/2024-01-19/vueling-implanta-reconocimiento-facial-viajes_3814339/, [retrieved on August 10, 2024].

[202] STONE, C.A. & Zissu, A. "Registered Traveler Program: The Financial Value of Registering the Good Guys," *Review of Policy Research*, vol. 24, nº. 5, 2007, pp. 446-448.

II. HISTORY OF THE USE OF BIOMETRICS IN THE FIELD OF DELINQUENCY

1. Advances in general biometrics

The identification of other people by their physical or behavioural traits is not a novel issue, since it is already present in the most elementary social organizations, the body being, par excellence, the principle of identity[203]. Human beings have always been able to recognize others through the senses. Biometric science did not develop until the second half of the 19th century with anthropometry, which is the origin of modern biometrics[204]. The latter began precisely in the field of crime, to which it contributes in the detection of criminals through the association of existing marks at a crime scene with those of individuals registered in a database, classifying the identity of individuals and selecting a subdivision of those from which it may come from[205]. The ways in which it can collaborate are many:

a) Increased efficiency and effectiveness of research since they can analyze evidence overcoming the limitations of human cognitive capabilities;
b) They provide a scientific basis and standardization for the crime investigation procedure through the analysis of large amounts of data that cannot be addressed by humans;
c) Visibility and documentation of analysis results[206].

The most common biometric systems have been based on the characteristics traditionally used by individuals for identification, including fingerprints and the face. However, over time, new mechanisms have appeared that take into account other elements, as we will discuss in this section.

[203] GIROTTO, S. "Il trattamento dei dati biometrici...", cit., p. 1237; JAIN, A.K. et al. "An Introduction to Biometric Recognition...", cit., p. 4. Since ancient times, human beings have been measured in order to use the data obtained in the elaboration of reference canons in architecture and sculpture ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales*..., cit., p. 45.

[204] In fact, the latter initially referred to studies specifically aimed at the dimensions of the human body, while the former alluded in general to studies of biological phenomena. It is not our task, as this is far from the objectives of the present study, to delve into the distinction between the two terms, nor into the process by which the term biometry began to be used instead of anthropometry. For more information on these issues, see in greater depth, ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales*..., cit., pp. 47-48.

For more on the historical evolution of biometrics over the last decades, see WAYMAN, J.L. "The scientific development of biometrics over the last 40 years...", cit., pp. 264-272.

[205] In the forensic context, a sample obtained from a crime scene is referred to as a crime scene sample, trace material and questioned item, while the reference sample that is compared to it is referred to as controlled material or known item. Some of these samples are collected physically while others are obtained digitally. SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification: Applications and Challenges", *Journal of Forensic Medicine*, vol. 1, nº. 1, 2016, p. 2.

[206] *Idem*.

The remote antecedent of the current biometric identification in this environment –namely, that developed in an automated way in the investigation of crime– is LOMBROSO, proponent of the Positivist School of Criminal Law. He, moving away from previous approaches that held that crime was the result of a free decision of the person who acts with an evil will, considered that he did so because of similar tendencies that have their origin in a physical and psychological organization different from a "normal" man. Thus, based on the study of "criminal anthropology"[207], he found a whole series of anatomical, biological and psychological characteristics that are no normal but common in "criminal man", many of which have an atavistic significance because they reproduce forms typical of the ancestors of human beings[208]. But not all delinquents share identical traits, which is why he made a classification, distinguishing between the anthropological or born delinquent (who presents evil instincts that he cannot change and, therefore, will commit a crime), occasional, insane, passionate and habitual[209]. To reach these conclusions, he studied a sample of criminals, from whom he took different anthropometric measurements, including the shape and size of the skull, height, weight, morphology of certain body parts such as ears or nose, among others[210].

Notwithstanding the above, the first milestone in the history of biometrics is the anthropometric identification system for criminals designed by Alphonse Bertillon, head of the criminal identification division of the Paris Police Department, who, at the end of the 19th century, presented the first system for identifying repeat offenders based on physical characteristics[211]. It was initially dedicated to classifying the shape of the nose, face or body. This technique proved to be effective when, two years after its implementation, 241 offenders were identified[212].

Bertillon elaborated a series of files on individuals in which, along with data relating to physical characteristics, he recorded personal information such as tattoos and scars as well as certain morphological characteristics such as hair and eye colour. This would be the basis for the design of the system known as *bertillonage*. It was not only a metric system, as it linked this information with other personal information. The method

[207] This branch of study was so called because it repeats the studies that general anthropology makes of the common man. LOMBROSO, C. *L'uomo delinquente. In rapporto all'antropologia, alla giurisprudenza ed alle disciplines carcerarie*, Napoleone Editore, Roma, 1971, pp. 45-46.

[208] The author goes so far as to compare these individuals to animals because he observed that some, such as certain types of horses, presented evil tendencies resulting from congenital cerebral or chronic alterations. He also likens them to savages because of their inferior physical and psychological structure and functions. *Ibd.*, pp. 7-ss.

[209] *Ibd.*, p. 47.

[210] *Ibd*., pp. 51 and next.

[211] JAIN, A.K. et al. "An Introduction to Biometric Recognition...," cit., p. 4.

[212] SERRATOSA, F. *La biometría para la identificación de las personas...*, cit., pp. 7-8. For the elaboration of the system, Bertillon used the information of eleven measurements of the head and body: height, width of the extended arms, sitting height, length of the head, width of the head, length of both ears, length of the left foot, length of the left middle finger, length of the left little finger and length of the left forearm.

described above became widespread in the West[213] but fell into crisis some time later, since it was observed that the measurements taken into account could vary with the passage of time and were not very unique[214], to which are added the difficulties related to the quality of taking measurements and because the metric units were different in some places[215].

Thus, the former was soon replaced by fingerprint research, partly because of the crisis it experienced after the "Will West case". In 1901 William West was imprisoned in Kansas and the Bertillon measures were taken. Two years later Will West was arrested and, likewise, the Bertillon measures were taken. The similarity of these as well as the features of the face led to think that they were the same person but later it was discovered that this was impossible because he was still imprisoned[216]. Therefore, only with the comparison of the fingerprints could it be determined that they were two different persons.

The recognition of the latter is one of the most important techniques for crime detection due to its robustness and uniqueness[217]. This, together with the realization that its collection, classification, storage and comparison was much more agile than the previous system, favoured its development[218].

Despite the above, although it became popular in the early twentieth century, when its use was accepted in forensic investigations[219], it has been used for criminal investigation purposes for hundreds of years. The first record was made in ancient China, when it was proved that some letters came from a particular person because the seals were engraved with the sender's fingerprint. In the 18th century it was observed that each person's fingerprints were different and could be classified into patterns such as arcs,

---

[213] ESCAJEDO SAN-EPIFANIO, L. *Biometric technology, identity and fundamental rights...*, cit., pp. 56-58.

[214] SERRATOSA, F. *La biometría para la identificación de las personas...*, cit., p. 10.

[215] ESCAJEDO SAN-EPIFANIO, L. *Tecnología biométricas, identidad y derechos fundamentales...*, cit., p. 58. Although it is true that the error rate is not known, nor is the percentage derived from the method and the lack of expertise of those taking the measurements.

[216] SERRATOSA, F. *La biometría para la identificación de las personas...*, cit., p. 11.

[217] SAINI, M., & KAPOOR, A.K. "Biometrics in Forensic Identification...," cit., p. 3.

[218] ESCAJEDO SAN-EPIFANIO, L. *Biometric technology, identity and fundamental rights*, cit., pp. 58-60. For the author, there is more myth than reality in the fact that the "Will West" case was the real trigger for the failure of Bertillon's method.

Although the latter was replaced by fingerprinting in forensic identification, the principle of converting the face into numerical data for the purpose of investigation and pattern recognition continues to be an underlying logic of how FRs work today. BUCHER, T. "Facing AI: conceptualizing 'fAIce communication' as the modus operandi of facial recognition systems", *Media, Culture & Society. Special Issue: Reclaiming the human in machine cultures*, vol. 44, nº. 4, 2022, p. 644.

[219] JAIN, A.K. & KUMAR, A. "Biometric Recognition: An Overview", in Mordini, E., & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal an Social Context*, Springer, 2012, p. 49.

In fact, the FBI has an automated fingerprint and criminal history identification system (IAFIS-Integrated Automated Fingerprint Identification System) which, as of 2016, had stored information on 70 million individuals in the criminal file, 31 million civilian fingerprints, and fingerprints of 73,000 known and suspected terrorists. SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification...," cit., p. 49.

whorls and loops. At the end of the 19th century, LEAs started to collect the fingerprints of criminals and already during the 20th century, fingerprint collection became routine and, today, it is possible to automate the process of fingerprint identification using computer systems[220], which makes it possible to make the comparison at least partially automated.

The above technique can be combined with others such as iris recognition to avoid some problems or limitations that may arise from the quality of the sample[221] , as it may happen, among other issues that they are deteriorated, incomplete or have been damaged by the environment or intentionally[222]. Focusing now briefly on the iris, it should be noted that the recognition of individuals through iris elements began in 1936 and from 1987 it began to be used for security purposes. However, it was not until 1994 that systems using mathematical algorithms were designed for this purpose. These applications are used, among other tasks, to facilitate authentication, border control and forensics. This system is not very invasive[223] and was used by the British Government from 2004 to 2013 in the program called "iris recognition immigration system" that allowed registered travellers to access the country through these facilities only with the automatic identification of this body part, without the need to present passports or any other means of identity verification.[224]

In the 1980s, the DNA system became popular as a verification mechanism using a computerized database. The use of this kind of information in criminal investigation has grown in recent years as it contributes to the identification of criminals and the solving of complex crimes. It is found anywhere on the body (i.e., hair, saliva, blood), so it can be easily detected at a crime scene[225]. Another technique used in criminal investigation, newer than the previous ones, is palm pattern recognition. It is considered very useful because it is permanent and unique to each person, even in monozygotic twins[226], in addition to the fact that about 30% of it is usually found at a crime scene[227]. Not only the handprint is used as a form of recognition, but also the dorsal veins. Systems for recognizing them began to be developed in the early 1990s and gained popularity in the

[220] HOPKINS, R. "An Introduction to Biometrics and Large Scale Civilian Identification...", cit. p. 348.

[221] This is the case in the model designed by SHREYA/CHATTERJEE. On it, see extensively, SHREYA, S. & CHATTERJEE, K. "Latent fingerprint and Iris fusion for enhancement of performance identification system", *Expert Systems With Applications*, vol. 235, 2024, pp. 1-15.

[222] HOPKINS, R. "An Introduction to Biometrics and Large Scale Civilian Identification...", cit. p. 347.

[223] SINGH, R. et al. "Implementation of iris recognition as a security measure against cyber crime in hyperledger fabric," *Semiconductor Optoelectronics*, vol. 41, no. 11, 2022, p. 443.

[224] SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification...," cit., p. 4.

[225] *Ibd.*, p. 3.

[226] GOH, M.K. et al. "Touch-less palm print biometrics: Novel design and implementation," *Image and Vision Computing*, vol. 26, nº. 12, 2008, p. 1551. The authors note some advantages of this technique compared to others: low-resolution images, low intrusion, stable line characteristics, and low-cost capture device. In addition, the palmprint covers a wider area than the fingerprint and is a rich source of useful information for recognition.

[227] SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification...," cit., p. 3.

2000s, although it was not until 2016 that the DL technique was introduced in this pattern. Since then, several automated systems have been developed that combine this with fingerprints and palm print to support robust identification[228].

Another feature that has been taken into consideration since 1999 for automated detection of individuals is the structure of the ear, which is considered useful due to the fact that the geometry and shape of this body part differs between individuals, in addition to the fact that it is easily visible in profiling and can be collected from video recordings or photographs[229].

It is not only through sight that we are able to identify others, but also through other senses such as hearing or smell[230]. In relation to the former, voice biometrics is used to determine the identity of an individual. Systems that have developed this function have been applied to the security field since the end of the 20th century and are useful because this parameter is linked to a particular subject[231]. Such identification mechanisms are often used when voice is the only feature available (i.e., in case of a bomb threat). The systems are capable of scanning thousands of voices and if the recording is of good quality, they will deliver a verdict quickly[232].

Those described so far are systems that fall into the group that we referred to in the first chapter as "strong biometrics" because they are anatomical-physical features of individuals that allow them to be identified –in some cases– univocally. However, in recent years, new techniques have emerged that fall into the categories of "weak biometrics" and "soft biometrics" because the parameters they use are less stable and individualizable, but together or fixed in a certain space and place, they collaborate in individual identification[233]. Some elements of the latter can be extracted from images of the face or facial movements, the body and others such as clothing. From them can be

[228] JIA, W. et al. "A survey on dorsal hand vein biometrics," *Patern Recognition*, vol. 120, 2021, p. 2.

[229] For more on the issue, ABAZA, A. et al. "A Survey on Ear Biometrics," *ACM Computing Surveys*, vol. 45, no. 22, 2013, pp. 1-35.

[230] In the latter case, a new emerging technology is based on odour biometry, since each object emits a characteristic aroma derived from its chemical composition, which allows it to be distinguished from others. This could be done with chemical sensors sensitive to a certain group of compounds. However, certain substances such as deodorants and perfumes could reduce the effectiveness. SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification...," cit., p. 4.

[231] MARKOWITZ, J.A. "Voice biometrics. Who are you? Your voice alone can be used to verify your personal identity-unobtrusively and invisibly", *Communication of the ACM*, vol. 43, nº. 9, 2000, pp. 66-67.

[232] Several systems have been developed based on voice identification in the criminal field. For example, AGNITIO's voice ID, which measures the biological features of a voice sample, through the actual sound of suspects' voices rather than the way words are spoken. Russia's Speech Technology Center developed the "VoiceGrid Nation," a system using advanced algorithms to identify voices that was subsequently exported to many other countries. SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification...", cit. p. 4.

[233] See in this regard, MORDINI, E. & TZOVARAS, D. (Eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012.

inferred issues related to gender, age and ethnicity, so they usually refer to demographic aspects[234].

In the field of criminal investigation, not only the former are used, but also the latter. For example, KLARE et al. proposed a method in which the attributes of the face are used to make an identification. These elements are extracted from sketches made after witness descriptions. The researchers defined 46 elements to extract all describable and durable facial points. Once established, they created an automatic feature extraction algorithm, which compares the sketch with images contained in police databases. After conducting a series of experiments, the designers concluded that the system could be applied in suspect detection, as it can achieve similar reliability to sketch recognition[235].

Another identifier that proves useful in surveillance is gait. This parameter can be used when other indicators such as the face have been surreptitiously altered to make identification more difficult. Thus, if there are recordings of the place where a crime has been committed, they can be analysed and the identity of the subject can be defined by means of this parameter[236]. Similarly, the manner of dress can be used for such purposes. The potential of this system has been demonstrated to substantially improve the results obtained by other soft biometrics, in addition to its effectiveness even in isolation[237].

As can be seen from the above, there are many biometric techniques and parameters used in the field of crime to identify suspected criminals or those who pose a threat to public safety. Increasingly, embedded systems, ambient intelligence and remote sensors are aggregating a wealth of data. The sources from which it is extracted are very diverse and can even come from personal social networks where users are constantly sharing images, audios and videos. This gives rise to risks especially to privacy and protection of personal data[238] among other rights, as we will have the opportunity to discuss in more detail below.

Thus, problems that were previously unthinkable arise from today's biometrics, such as the data on which it is based, the way in which it is collected and its management. It is now possible to collect increasingly intimate information, using particularly invasive instruments in the personal sphere, storing it in databases that can be interconnected[239] and even lead to the creation of profiles used for commercial purposes.

This technology shows great potential in certain locations such as airports, stadiums, defence facilities, as well as in industry and companies where security and

[234] To learn more about these biometric identification systems, see NIXON, M.S. et al. "On soft biometrics...", cit., p. 218-228.

[235] KLARE, B.F. et al. "Suspect Identification Based on Descriptive Facial Attributes," *IEEE International Joint Conference on Biometrics*, 2014, p. 1-8.

[236] SAINI, M., & KAPOOR, A.K. "Biometrics in Forensic Identification...," cit., p. 4.

[237] NIXON, M.S. et al. "On soft biometrics...," cit., p. 225.

[238] ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit., p. 2.

[239] GIROTTO, S. "Il trattamento dei dati biometrici...", cit. p. 1238.

privacy are required[240]. The major impetus for the development of biometrics has been the growing threat of terrorism and crime, since, as we discussed in the corresponding section of the previous chapter, these are two problems of particular concern because of the serious consequences they entail, as well as the increased reliance on information networks for communication and commerce. In such cases, it is considered necessary to be able to establish and monitor the identity of individuals, and the security benefits that can be derived from these mechanisms must be weighed against the harm[241].

However, despite the rapid development and growth of biometric technology, there are some concerns about recognition accuracy due to the large populations involved, privacy and security breaches, among others. These systems are not infallible and, particularly in the area of the latter, it has become evident that the promise of "uniqueness" with which biometrics is often associated can be undermined by fraudsters who could fool the systems through mimicking physiological or behavioural characteristics, sometimes with surprising ease[242]. These problems and challenges must be countered if applications are to perform effectively. To address them, it will be necessary to tackle different strategies from the technological, social and legal domains.

Despite these drawbacks, the decision was taken within the EU to incorporate biometric data into citizens' passports and the control of asylum seekers. This led to the rapid implementation of such systems in a multitude of scenarios, such as cross-border judicial cooperation[243]. In addition, biometrics are now increasingly being used by LEAs for surveillance purposes with the implementation of CCTVs with embedded FRs. In an attempt to address the problems arising from the sometimes irrational expansion of biometrics and to ensure that existing fundamental rights legislation is respected, the EU has enacted the AIA.

Due to the controversy raised by the latter's regulation of RBIS in public spaces in terms of law enforcement, as well as the practical relevance that such mechanisms have

[240] DROSOU, A. & TZOVARA, D. "Activity and Event Related Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 130.

[241] Such damages may derive from a disproportionate increase in Big Data practices, the heterogeneity of data sources, formats and quality of information that may impact on issues related to the accuracy of biometric data supporting criminal evidence, seriously affecting the rights of individuals. The diversification and increased use of these techniques also increases the sensitivity of the data and the risk of adverse impacts on the affected subjects when the security and confidentiality of processing is shown to be insufficient. There may also be issues related to opacity and lack of predictability. ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit., p. 3.

[242] DERAVI, F. "Intelligent Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p. 178.

[243] It has created a European search portal, a shared biometric matching service, a common data registry, based on archived biographic and biometric data from various systems. TINOCO PASTRANA, A. "La modernización de la cooperación judicial transfronteriza en la Unión Europea: la implementación de la digitalización", *Revista Asociación de Profesores de Derecho Procesal de las Universidades Españolas*, nº. 8, 2023, p. 128.

in the field of criminal investigation and security[244], our analysis will focus on them, despite the interest raised by the study of the other biometrics discussed in this section.

2. Approach to the evolution and operation of facial recognition systems

The earliest known work on automated face recognition –although not all stages of the process were automated– dates back to 1964 and was carried out by BLEDSOE at the *Panoramic Research Institute* in Palo Alto, California. The initial approach he followed was to manually mark various landmarks on the face, which could be mathematically rotated by a computer to compensate for differences that might arise from variation in the individual's pose. The distances between marks and proportions could be automatically computed and compared to determine goodness of fit. It was noted that there were differences and difficulties in comparing images when the rotation of the face differed, the brightness was not the same, or the expression changed[245]. Subsequently, many other investigations were developed in this sense but we will not address all of them, as this work is far beyond the scope of our study. For this reason, we will focus on those that, in our opinion, represented a significant advance in the development of FRs up to the current situation[246].

Thus, the first fully automated facial identification system was deployed in 1973. The researchers used a top-down control strategy driven by a generic model of expected features. The system computed a set of face parameters (eyes, nose, mouth, etc.) from a simple image and used a pattern classification technique to identify the face within a known set[247]. Ten years later, SIROVICH/KIRBY began to apply linear algebra to face recognition. They calculated a coordinate system for image compression, where each coordinate corresponds to one of them. They started from the assumption that each face can be represented through certain elements or features. This technique was called *eigenpictures*[248] and the researchers assumed that only a small number of elements were sufficient to identify face images. They further understood, at least in principle, that each

[244] In this regard, among others, TURK, M. & PENTLAND, A. "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, vol. 3, nº. 1, 1991, p. 71; MIAN, A. et al. "Keypoint Identification and Feature-Based 3D Face Recognition", in LEE, S.W. & LI, S.Z. (Eds.), *Advances in Biometrics. International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, p. 163; & TASKIRAN, M., et al. "Face recognition...", cit., p. 1.

[245] BLEDSOE, W.W. "Man-Machine facial recognition: Report on a large-scale experiment," *Technical Report PRI:22*, Panoramic Research Inc. Palo Alto, CA, 1966.

[246] For a more in-depth account of the inception and subsequent development of the technique, see extensively, TURK, M. & PENTLAND, A. "Eigenfaces for Recognition...", cit. p. 72.

[247] KANADE, T. "Picture Processing System by Computer Complex and Recognition of Human Faces", *Department of Information Science*, Kyoto University, 1973. For more on the system at a general level, see also SAKAI, T. et al. "Picture Processing System Using a Computer Complex", *Computer Graphics and Image Processing*, vol. 3, 1973, pp. 207-215.

[248] The *eigenpictures* are understood as the *eigenfunctions* of the mean covariance of the sample of faces. SIROVICH, L. & KIRBY, M. "Low-dimensional procedure for the characterization of human faces", *Optical Society of America*, vol. 4, nº. 3, 1987, p. 519.

collection of facial images could be approximately reconstructed by storing a small sample of measurements for each face and a small set of standard images. The idea behind the model is that, just as humans are able to store and recognize many faces instantaneously, such a function could also be performed in the digital domain. To develop their project, they took a sample of one hundred and fifteen images of male students at Brown University. This process began as a search for a low-dimensional representation of facial images, and the authors concluded that feature analysis on a collection of them could form a basic feature set. They also showed that few values (less than a hundred) were required to accurately encode a normalized facial image. Added to the above was the finding that the error rate arising from changes in illumination was low[249].

This approach was followed by TURK/PENTLAND, who in 1991 went further and designed a system that could detect faces within images, which led to the first cases of automatic face recognition. The authors named the small elements into which the images are decomposed as *eigenfaces*[250], which would be the main components of the set of facial images that make up the set intended for initial training. With them, they intended to extract the relevant information from the face, encode it efficiently and compare an encoded face with those contained in a database. From this approach it is understood that each subject can be represented exactly by a linear combination of *eigenfaces* and that not all parameters of the face are needed to recognize it, but only the best ones are sufficient[251]. They considered that if a multitude of facial images can be reconstructed by weighted sums of a small collection of feature elements or *eigenpictures*, perhaps an effective way to learn to recognize faces would be to construct the feature elements by experience gained over time and to recognize particular faces by comparing the feature weights needed to reconstruct them with the weights associated with known individuals. Each would be characterized by the *eigenpicture* required to describe and reconstruct them[252]. For the design of the instrument they understood that, if the instrument was

[249] *Ibd.*, pp. 519-524. The authors took into account for this study only elements of the eyes and nose. Later they extended to the full face by including also parameters of the mouth, arriving at similar results. KIRBY, M. & SIROVICH, L. "Application of the Karhunen-Loève Procedure for the Characterization of Human Faces", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 1, 1990, pp. 103-108.

[250] TURK, M. & PENTLAND, A. "Eigenfaces for Recognition...", cit., pp. 73-74. The authors use this term to refer to the vectors of the covariance matrix corresponding to the original images of the face, having the appearance of a real one. The initial idea is to find the principal vectors that best represent the distribution of the face images within the entire image space. These vectors define the subspace of the face images, called "face space".

[251] The features they extract from the face are linked directly or not to those elements that are identified with our intuitive notion of what makes up a face: eyes, nose, lips and hair. In mathematical terms, the researchers' goal was to find the principal components of the distribution of the faces, or the *eigenvectors* of the covariance matrix of the image set, treating the images as one point in a much larger dimensional space. These *eigenvectors* are ordered by taking into account the different amount of variation between facial images and can be understood as a set of elements that together characterize the variation between face images. Each image location contributes more or less to each *eigenvector*, which is why they understand this to be a type of ghost face that they call *eigenface*. *Ibd.*, p. 73.

[252] To learn more about the operations and steps followed, as well as how the *eigenfaces* are calculated, see *Ibd*, pp. 73-76.

intended for a small group of individuals, the sample required would be similarly small. However, if it is intended to represent many people or to learn new faces, a larger set of faces is needed[253].

In our opinion, there are several important findings about this mechanism in relation to our object of study. Firstly, the ability to recognize images even in motion; secondly, the ability to learn to recognize new faces in an unsupervised way. At this point, when an image approaches a face space but is not classified as familiar, it is labelled as "unknown". The computer stores the vector pattern and the corresponding unfamiliar image that will be recognized as a new unidentified face. The corresponding images are then checked for similarity to the group patterns. If the images pass the similarity test, the average of the feature vectors is added to the database of known faces. Occasionally, *eigenfaces* can be recalculated using these stored images as part of the new training set[254]. Third, note that the system they created can locate and identify faces in near real time in an uncontrolled environment. Recognition then occurs at speeds of up to two or three times per second. When a face is recognized, the image of the identified subject is displayed on the monitor[255]. Finally, the last major achievement of the system is linked to the neural networks with which the *eigenfaces* would be implemented using simple elements of parallel computing[256].

Currently, studies on FRs divide them into two main groups: *image-based* and *video-based methods*. The systems included in the former aim to recognize a person using physical appearance (and can be of three types: *appearance-based (holistic) methods*, *model-based methods* and *texture-based methods*). On the other hand, the latter use the appearance as well as the changes that occur in it over time or the dynamics of the face and, in turn, are divided into *set-based methods*, which treat the fragments of a video sequence as a collection of images without paying attention to the temporal order of the sequences; and *sequence-based methods* that use the aforementioned sequences but maintaining the temporal order. Thus, the dynamics of the face over time also play an important role in person recognition[257].

[253] *Ibd.,* pp. 76-77.
[254] *Ibd.,* p. 79.
[255] *Ibd.,* pp. 81-82.
[256] *Ibd.,* p. 83. In this case, the input layer receives the image of the input face, with one element per pixel. The weights from this layer to the hidden layer correspond to the *eigenfaces*, so the value of each hidden unit is the scalar point of the input image and the corresponding *eigenface*. The output layer produces the face space projection of the input image when the output also corresponds to the *eigenfaces*. These networks implement a learned stimulus-response mapping, where the learning phase modifies the connection weights. An auto associative network implements the projection in face space. Similarly, reconstruction using *eigenfaces* can be used to remember a partially occluded face.
[257] For a more in-depth knowledge of all the systems that have been developed within each category, see in greater depth, TASKIRAN, M. et al. "Face recognition...", cit., pp. 3, 7-18, who carry out a systematic review of all the studies on FRs carried out up to 2020 and extensively expose all the perspectives and mechanisms developed within them.

Within *appearance-based face recognition*, DL or DNN methods stand out[258], which have been particularly successful in the FR domain, where contemporary deep models report near-perfect performance on popular and long-running benchmarks such as the *Labeled Faces in the Wild* (LFW) database[259]. Moreover, their use is much more widespread than that of other methods, in part because of increased processing power and the collection of large databases containing multiple samples[260].

The *DeepFace* model is one of the systems framed within DNN. TAIGMAN et al. in 2014 described the practical application of this system, which includes a 3D analytical modelling of the face based on landmarks that is used to transform a detected facial cut-out into a 3D frontal model. The approach used by the aforementioned authors relies on landmark detectors to drive the alignment process. The face recognition rate demonstrated by the system is approximately 97.35% in LFW[261]. This database was created to study the FR problem in free environments. Its main contribution was to provide a large set of face images in relatively uncontrolled environments with the variations observed in everyday life (pose, lighting, gender, age, race, dress style, hair style, camera quality, colour saturation, etc.)[262]. Since its implementation, the accuracy of the system reached 99.80% in just three years[263]. However, although the DDN mechanisms[264] offer fairly high accuracy rates in identification and verification, their robustness under adverse conditions is not as high, such as when images are not of high

[258] DL has reshaped the scope of FR study in almost all aspects such as algorithm design, training/testing datasets, application scenarios, and even evaluation protocols. DL methods such as convolutional neural networks (CNNs) use a multi-layered cascade of processing units for feature extraction and transformation. They learn different levels of representations corresponding to different levels of abstraction. The levels form a hierarchy of concepts, showing strong invariance to changes in face pose, brightness and expression. In CNNs the lower layers automatically learn features in a manner similar to Gabor and SIFT designed over decades, while the higher layers learn at a higher level of abstraction. Finally, the combination of these higher levels of abstraction represents facial identity with unprecedented stability. WANG, M. & DENG, W. "Deep face recognition: A survey", *Neurocomputing*, vol. 429, 2021, p. 216.

[259] GRM, K. et al. "Strengths and weaknesses of Deep learning models for face recognition against image degradations," *IET Biometrics. Special Issue: Face Recognition and Spoofing Attacks*, vol. 7, nº. 1, 2017, p. 81.

[260] TASKIRAN, M. et al. "Face recognition...", cit., p. 8.

[261] The proposed face representation was obtained from a large collection of Facebook photographs, known as the Social Face Classification dataset. Subsequently, the representations are applied to the LFW, which is a *de facto* reference dataset for face verification in uncontrolled environments, and to the Youtube Faces database, which is modeled similarly to the LFW but in this case focuses on video clips. TAIGMAN, Y. et al. "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, pp. 1701-1708.

[262] HUANG, G.B. et al. "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments", *Workshop on faces in'Real-Life'Images: detection, alignment, and recognition*, 2008, pp. 2-5. This database is very interesting because the FR operates in real-world situations where one has little (or no) control over the composition or the images are pre-existing (e.g., availability on the Internet), so the development of recognition algorithms capable of handling such data is very beneficial for information retrieval and data mining. Other similar databases exist but vary in size, scope and purpose.

[263] WANG, M. & DENG, W. "Deep face recognition...", cit., p. 216.

[264] There is a wide variety of DL architectures or systems applied to Deep FR. To learn more about all of them and their evolution, *Ibd*, pp. 221-225.

quality and there are variations in illumination or noise[265]. For this reason, more research should be done to improve such weaknesses of FRs using DL techniques.

Systems based on the latter type have three main phases[266]:

1) *Face pre-processing*. The need for face pre-processing is necessary in view of the problems related to the robustness of the recognition, since there are variations when the conditions of luminosity, subject position and facial expressions change in uncontrolled environments (as we have just explained above). There are two approaches to try to control this situation. On the one hand, the so-called *one-to-many augmentation* that generates many patches or images of pose variability from a single image to allow deep networks to learn invariant representations of that[267]. The goal is to make the Deep CNN invariant by creating recreations of the face in different positions from a single image during training. This is done because it is costly in economic terms and time consuming to collect a large set of images to create the training database[268]. On the other, the *many-to-one normalization* pre-processing

[265] See in this regard, GRM, K. et al. "Strengths and weaknesses of Deep learning models...", cit. pp. 84-88. Similarly, CHEN, S. et al. "Face Recognition from Still Images to Video Sequences: A Local-Feature-Based Framework," *EURASIO Journal on Image and Video Processing*, vol. 2011, 2011, p. 2.

[266] TASKIRAN, M. et al. "Face recognition...", cit., pp. 8-9.

[267] WANG, M. & DENG, W. "Deep face recognition...", cit., p. 217.

[268] Within this approach there are three different methods. The first uses *data augmentation methods* such as photometric and geometric transformations. On that one, see, KRIZHEVSKY, A. et al. "ImageNet Classification with Deep Convolutional Neural Networks," *Advances in neural information processing systems*, vol. 25, 2012, pp. 1-9. The database they used contained images of varying resolution, while their system requires constant dimensions. Therefore, they performed image pre-processing by resizing the images. As examples of methods using geometric transformations in the pre-processing stage, XIE, S. & TU, Z. "Holistically-Nested Edge Detection", *Proceedings of the IEEE International Conference on Computer Vision*, 2015, pp. 1395-1403. The researchers use natural images to develop their model. The system automatically learns the type of elements that are essential if it is to approach human ability to resolve edge detection ambiguity in natural images and object boundaries. The aim is to create a deep network to effectively generate multilevel elements and have several stages with different steps to capture the intrinsic scales of linear maps. They concluded that pre-processing is useful in low-level image detection task; and YANG, J. et al. "Weakly-supervised Disentangling with Recurrent Transformations for 3D View Synthesis," *Advances in neural information processing systems*, vol. 28, 2015, pp. 1-9. In this case, the researchers dealt with the problem of synthesizing novel views of a 3D object from a single image. They understood that by focusing attention on the particular object, extensive training data can be collected. One of the main conclusions they reached was that increasing the length of the training sequence improves the model's image prediction performance.

The second approach is based on the reconstruction of a 3D model of the face from which 2D images in different poses are subsequently created. MASI, I. et al. "Rapid Synthesis of Massive Face Sets for Improved Face Recognition," *12th IEEE International Conference on Automatic Face & Gesture Recognition*, 2017, pp. 604-611. Aware of the problems arising from the creation of large databases containing a lot of information of the same person, especially in terms of high cost, they propose a simple and efficient method to represent faces in multiple perspectives. They concluded that a large number of faces in a database is not necessary for the identification to be effective.

Finally, in the third one, CNN models are used to create 2D images directly instead of creating 3D models from those and projecting them back into 2D images of different poses. QIAN, Y. et al. "Task Specific Networks for Identity and Face Variation," *13th IEEE International Conference on Automatic Face on Automatic Face & Gesture Recognition*, 2018, pp. 271-277. In addition, the above research takes into account the possible variations that can happen due to the change in certain conditions that influence the quality of recognition, such as illumination.

approach recovers the canonical view of face images from one or several images of a non-frontal view, so that the FR can be performed as if under controlled conditions[269]. The purpose is to generate the face view using images obtained from different angles in uncontrolled environments[270]. For its part, GAN is a model that straddles the two previous ones and is gaining attention in both. In this case, what the system does is to break the constraint that face synthesis must be done in a supervised manner[271].

2) *Deep feature extraction*. In this second stage, the most important decisions focus on the choice of architecture and loss function, and some issues need to be solved in order to improve the efficiency of the system[272].
3) *Face matching*. Once the selected architecture is trained using the given function loss and data training, deep factor extraction can be performed for data testing, as well as for face identification and verification operations[273].

Other methods included in *video-based face recognition* are interesting for our object of study[274], since the images used are obtained from video surveillance cameras. Thus, *super-resolution* and *cross-resolution methods* use low-resolution images extracted from such systems to, once the information has been collected, obtain a high-resolution image[275]. This process is important since the images of faces obtained from such mechanisms are of low quality and usually occupy a small portion of the screen, which makes it challenging for both the computer and the human operator to properly identify a subject from the database[276]. GUNTURK et al. argue that the situation of low resolution

Very interesting is the work of BAO et al. who used Generative Adversarial Networks (GAN) to realistically synthesize faces regardless of whether the individual's information was recorded in the database or not. It allowed using large amounts of unlabelled face data to improve the fidelity of faces that were not included in the database. BAO, J. et al. "Towards Open-Set Identity Preserving Face Synthesis," *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 6713-6722.

[269] WANG, M. & DENG, W. "Deep face recognition...", cit., p. 218.

[270] Different systems have been used within it. For more information on this subject, see TASKIRAN, M. et al. "Face recognition...", cit., p. 8.

[271] WANG, M. & DENG, W. "Deep face recognition...", cit., p. 225.

[272] TASKIRAN, M. et al. "Face recognition...", cit., p. 8. Feature extraction poses a special challenge for the one-shot face recognition problem, which refers to the case where there is only one image of an individual in the gallery. This issue is difficult because it is complicated to represent variations in the data with few samples.

[273] *Ibd.*, pp. 8-9. The main results obtained show the success of the FR using different systems and databases. Over the years, the accuracy of recognition has increased.

[274] We omit from our presentation those that deviate from face recognition in the field of security surveillance and crime prevention. However, we must point out that they have obtained very good results in terms of accuracy, as is the case with the *frame-selection based methods* and *sequence-based face recognition*. *Ibd.*, 15-17.

[275] LIN, F. et al. "Super-Resolved Faces for Improved Face Recognition from Surveillance Video", in LEE, S.W. & LI, S.Z. (Eds.), *Advances in Biometrics. International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, p. 2. On p. 8 of the same paper, the authors consider that a fully automated recognition system was at that time impractical. To increase efficiency, the surveillance system will need to operate in a semi-automated fashion by generating a list of top matches for subsequent human recognition.

[276] TASKIRAN, M. et al. "Face recognition...", cit., pp. 1-2. A human operator is usually responsible for monitoring images from several cameras simultaneously, which increases the possibility of errors. One solution to this problem, the authors argue, would be to complement the natural ability to recognize images with the ability of computers to process large video data sets.

images is especially critical in surveillance scenarios where often only low resolution video footage is available. It is a critical issue in this domain where one works with real-time systems where a high-resolution algorithm is expected to work on continuous video streams. In such a case, the researchers propose a method based on increasing resolution to extract only the necessary facial information. This resulted in a significant reduction of the computational complexity[277]. To overcome the problems arising from the low resolution of images in surveillance systems, *3D face modeling* methods have been proposed.

A model framed in the latter system is the one developed by PARK/JAIN, which helps to increase the hit ratio by reconstructing a 3D facial model from multiple non-frontal video frames, generating a frontal view of the derived 3D model and using a commercial 2D recognition engine to recognize the synthesized frontal view. This mechanism allows identifying individuals in a video that mostly contains non-frontal faces, assuming that only the frontal image is in the data gallery[278]. Finally, *manifold methods* attempt to model face subspaces directly without paying attention to the underlying physical image formation process.

A significant study within the latter was conducted by CHEN et al., who compared four different methods using LFW *image-based* and MOBIO *video-based* databases, concluding that systems based on the latter are more successful in hostile conditions than those based on the former[279]. To develop their research, the authors started from the assumption that CCTV images are recorded without monitoring and the videos are mainly used for post-crime forensic analysis, so they are not able to provide an adequate response to the crime problem. For that reason, they considered it necessary to detect events and subjects from the CCTV before the offenses take place, which means that the cameras should always be monitored. This task is difficult to be carried out by individuals, since only a limited number of cameras can be monitored simultaneously and, due to the large number of cameras in existence, it would require a lot of personnel resources, resulting in an excessively high cost. Added to this is the problem of reduced attention span when a task is performed over a long period of time. Advanced surveillance systems that use

In the field that concerns us, that is, the maintenance of security through the identification of suspected criminals or terrorists, the quality of the image is very important, in order to avoid that the mechanism does not identify or does not correctly identify the individual being searched for. What happens in uncontrolled environments is that the image quality decreases due to a variety of factors such as changes in lighting, poses, etc. Therefore, the results of the mechanisms are often not correct. This issue was echoed in 1999 by BURTON, A.M. et al. in their study "Face recognition in poor-quality video: Evidence form security surveillance", *Psychological Science*, vol. 10, no. 3, 1999, p. 243.

[277] GUNTURK, B.K. et al. "Eigenface-Domain Super-Resolution for Face Recognition," *IEEE transactions on image processing*, vol. 12, nº. 5, 2003, p. 597-606.

[278] PARK, U. & JAIN, A.K. "3D Model-Based Face Recognition in Video", in Lee, S.W., & Li, S.Z. (Eds.), *Advances in Biometrics International Conference ICB 2007, International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, pp. 1085-1094.

[279] CHEN, S. et al. "Face Recognition from Still Images to Video Sequences...", cit. pp. 6-10.

computers to monitor video and alert human operators to respond are therefore seen as a possible solution.

The researchers implemented the FR mechanism in crowded environments such as train stations using existing cameras. Their approach, unlike similar ones, was shown to be effective in face recognition in the surveillance domain using local facial elements, being able to handle the recognition of low-resolution images and with variations in illumination, pose and expression, not being sensitive to localization errors. Moreover, the computation of this approach is fast enough to perform real-time processing[280]. Another mechanism acting in real time is the one proposed by LIU et al. which is even able to simultaneously detect several faces even if there are variations in the position of the head or the face is not completely visible and occluded[281].

For a number of reasons, such as the fact that it is done remotely without interaction with the individual, FR technologies have been observed to have extensive benefits compared to other parameters such as fingerprinting. Particularly for law enforcement purposes, this mechanism can help identify individuals with criminal records or who have other legal problems with the justice system. Officers tasked with this function can use the face to compare images of suspects in databases to support investigations[282]. Thus, they have been inserted into various environments for such purposes.

Warfare is one of them. In the spring of 2010, the Canadian Armed Forces began using a surveillance device called Handheld Interagency Detection Equipment (HIDE) to fight the Taliban and members of Al-Qaeda. Canadian soldiers began collecting facial images of Afghans along with other biometric data such as iris and fingerprints. Once collected, they were transferred to a massive central database. The system informed personnel within minutes if an individual was suspected of being a threat to the NATO-led International Security Assistance Force[283]. Some benefits of face biometrics in warfare are highlighted: effectiveness, reliability and convenience. The results show an increase in the security of the forces that use them, facilitating the killing or capture of enemies and detecting threats[284]. However, like all FRs, it presents a series of risks[285] linked to privacy, identification errors and inappropriate use of the data.

[280] *Ibd.*, pp. 1, 5.

[281] LIU, R. et al. "Tracking and Recognition of Multiple Faces at Distances", in Lee, S.W. & Li, S.Z. (Eds.), *Advances in Biometrics. International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, pp. 513-522.

[282] MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU*..., cit., p. 3. Other areas in which the technique has been introduced are consumer applications, business and payment applications, among others such as digital marketing, health, etc.

[283] For more on how the technique developed in this context, see, MITCHELL, A. "Distinguishing friend from foe...", cit., pp. 289-330.

[284] *Ibd.*, pp. 295-297.

[285] *Ibd.*, pp. 298-304.

The increased attention that FRs have received is also due in part to the good results observed when they have been inserted in surveillance and access control systems in certain areas[286], such as airports. In this regard, we mention the AURORA-AI mechanism, installed in large airports such as London Heathrow and Manchester. It has three main functions: identification, prediction and detection. For the purposes of our research, the most interesting is the first one, since it is linked to the recognition of individuals at a distance. This instrument combines its own FR software with specialized near-infrared sensors. The latter make it possible to avoid problems associated with changes in lighting conditions[287]. In the UK, since 2017 the South Wales Police carried out an "AFR Locate" project for events such as the Champions League final, international rugby matches, concerts, etc. Images were captured, automatically processed and checked against people on watchlists[288]. The implementation of such systems was controversial and the subject of prosecution by the *High Court of Justice Queen's Bench Division. Divisional Court Siting at Cardiff Civil Justice Center. Case R (Bridges) v CCSWP and SSHD*, the details of which will be set out more fully below.

After the 9/11 attacks, there was an urgent need to increase security due to the threat posed by a new form of terrorism that was previously unknown. This need is particularly noticeable at large events that bring together large numbers of people, such as sporting events, which are a privileged space for terrorists. Thus, in the 2001 Super Bowl final, FRs were included as a security measure that detected the faces of spectators and tried to match them with those collected in police databases of terrorists and known criminals[289]. In the soccer field, it has been implemented since 2017 in several stadiums in Uruguay, where it contributes to the identification of individuals who are not authorized access to matches[290].

In the same year, for the G20 meeting in Hamburg, Germany, a FRs was deployed from recordings for crime detection and investigation[291]. In Berlin in 2019, a similar system was deployed to detect suspicious behaviour at the Südkreuz train station.

[286] PARK, U. & JAIN, A.K. "3D Model-Based Face Recognition in Video...", cit. p. 1085.

[287] *Aurora-AI*. Electronic resource obtained via the World Wide Web: https://aurora-ai.com/, [retrieved on March 10, 2024].

[288] COTINO HUESO, L. "Automated facial recognition and biometric identification systems under the overlapping regulation of Artificial Intelligence and Data Protection...", cit., p. 348. Its use was advertised on posters and warned in social networks. In 2019 the courts considered it appropriate, although the Data and Transparency Authority in 2021 noted its inappropriate use.

[289] WOODWARD, J.D. *Super Bowl surveillance....*, cit. p. 3.

[290] LA VANGUARDIA, "Comunicado: facial recognition in Uruguayan soccer," April 26, 2018. Electronic resource obtained through the Web: https://www.lavanguardia.com/vida/20180426/443015024931/comunicado-reconocimiento-facial-en-el-futbol-uruguayo.html, [retrieved on 10 March 2024]; & NARANJO, J.C. "Reconocimiento facial, ¿el fin de la violencia en los estadios de fútbol?", *Crónica de Deportes*, 1 May 2018. Electronic resource obtained via the Web: https://cronicaglobal.elespanol.com/deportes/reconocimiento-facial-violencia-estadios-futbol_138041_102.html, [retrieved on 10 March, 2024].

[291] COTINO HUESO, L. " Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de Inteligencia Artificial y Protección de Datos...", cit., p. 348. The Hamburg data authority initially considered it inadmissible, but a court overturned the suspension and it is pending in the courts.

Previously, between August 2017 and July 2018, a pilot project was developed at that station, driven by the Home Office, the federal and state police, also with the support of a train company in the country. The results of the study determined a high efficiency in face detection when three different systems were combined, but not separately[292].

The city that pioneered the installation of these systems in uncontrolled environments was London in October 1998, specifically in the borough of Newham, and just three years later the system had been implemented in 300 CCTVs linked to a London Metropolitan Police Service control room. That same year, the FaceIt system began to be used in Birmingham to identify known criminals or criminal suspects with an arrest warrant. In 2002, the Virginia Beach police department deployed FaceIt on its CCTV systems, whose functions were not limited to those listed above, but extended to locating missing persons[293]. In France, the Nice police developed a test of live facial recognition technologies at the 2018 carnival. The purpose was to test their efficiency. The data used were from volunteers. In addition, event attendees could choose to enter or not enter the area where the FR technologies were being used. The French Gendarmerie has made use of such systems in criminal investigation but not in real time due to the absence of a legal basis for this[294].

Despite the laudable purposes for which it was initially used, there is a risk that it may be extended to other purposes for which it was not intended and whose insignificance does not even make it advisable, such as petty crime. It may even collaborate with the development of a mass surveillance system, as in China occurs, where systems allow static and dynamic facial detection[295]. One of the objectives pursued by the Chinese government is to monitor millions of Muslim and ethnic minority citizens[296].

Continuing with Asia, since 2018 Singapore has been considering installing cameras equipped with FRs on its 110,000 streetlights for purposes such as assisting in anti-terrorist operations. The system is part of the "Lamppost as a Platform" project that began in 2019, with the aim of collaborating with authorities to recognize faces in the crowd and thereby increase security. These lampposts have more functions, but for our

[292] EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance at Berlin-Südkreuz," *Internet Policy Review. Journal of Internet Regulation*, vol. 9, nº. 1, 2020, pp. 2-7.

[293] BREY, P. "Ethical aspects of facial recognition systems in public places", *Journal of Information, Communication and Ethics in Society*, vol. 2, nº. 2, 2004, p. 100.

[294] FRA, *Facial recognition technology: Fundamental rights considerations in the context of law enforcement*, 2020, p. 12.

[295] TORRES LÓPEZ, L.S. & PERALTA GUTIÉRREZ, A. "Police use of Artificial Intelligence Systems...", cit., p. 473.

[296] VIDAL LIY, M. "“2,5 millones de personas en China, bajo el control de una empresa de vigilancia facial", *El País*, February 18, 2019. Electronic resource obtained via the World Wide Web: https://elpais.com/internacional/2019/02/17/actualidad/1550422679_515333.html, [retrieved on 11 March 2024]; & COLLINS, J. "China is using facial recognition to track millions of Muslim citizens wherever they go," *Quartz*, 17 February 2019. Electronic resource retrieved from World Wide Web: https://qz.com/1552708/china-is-using-facial-recognition-to-track-millions-of-muslim-citizens-wherever-they-go/, [retrieved on 11 March 2024].

object of study, the aforementioned FR stands out, with which it is intended to count and analyse crowds, as well as to help in the public spaces security.

It is not only in the latter that such technology has been used, given that since 2017 it has also been implemented together with iris recognition technology at Changi Airport for airport control and boarding, the latter being carried out automatically. The justification for this lies in the greater agility and reliability compared to human control[297]. Not only that, but the country also launched a facial verification program as part of its national digital identity program, being a world pioneer[298]. Another system developed in Korea is called ETRI, which, through the permanent capture of images in public spaces, aims to determine the possibility of committing crimes by means of behavioural analysis of the subjects circulating in them. For the development of this application, images of real crimes are used through an ML system that makes it possible to establish behavioural patterns associated with criminal activity[299].

The situation described is happening in countries that are not close to our socio-cultural environment, but what happens in those that are close to us or even in the context of the EU in general. In the later, the application of FRs is not free of controversy and associated problems, especially with regard to the possible infringement of citizens' rights and freedoms. In this regard, in Sweden in 2021, the Data Authority imposed a fine of €248,218 on police officers for the illegal use for police and investigative purposes of the FR application Clearview AI, which has three billion images from social networks and websites. With it, the agents intended to find out if the person represented in the image matched others collected in the database. The Authority emphasizes that the police did not implement sufficient organizational measures to ensure and be able to prove that the processing of personal data was carried out in accordance with the GDPR. Therefore, it considers that the biometric data was unlawfully processed for facial recognition and a required data protection impact assessment could not be carried out[300].

Another case, this time in Italy arose when the *Sistema Automatico di Riconoscimento Immagini (SARI)* began to be used in 2019 in public places for the

[297] KAI YI, W. "No need to scan Passport for immigration clearance at Changi Airport's T4 in contactless trial," *The Straits Times*, 4 December 2019. Electronic resource retrieved from World Wide Web: https://www.straitstimes.com/singapore/transport/contactless-immigration-trial-extended-to-changi-airport-t4, [retrieved on 2 April, 2024].

[298] ALMOGUERA, P. "Singapur estrena un sistema de verificación facial como DNI," *El País*, October 20, 2020. Electronic resource obtained through the Web: https://elpais.com/retina/2020/10/02/innovacion/1601653052_245522.html, [retrieved on April 2, 2024]. See also, TORRES LÓPEZ, L.S. & PERALTA GUTIÉRREZ, A. "Uso policial de sistemas de inteligencia artificial...", cit., pp. 474-475. The authors go on to state that the system uses a biometric authentication technology in the cloud that not only confirms the user's identity, but also verifies that it is a real person and not a photograph or mask. It is not an identification mechanism, but a verification mechanism, so it acts with the consent of individuals and is subject to intense data protection regulations.

[299] TORRES LÓPEZ, L.S. & PERALTA GUTIÉRREZ, A. "Uso policial de sistemas de inteligencia artificial...", cit., pp. 475-476.

[300] Swedish Privacy Authority, February 10, 2021, DI-2020-2719. Electronic resource obtained via the Web: https://gdprhub.eu/index.php?title=IMY_(Sweden)_-_DI-2020-2719, [retrieved on 3 April, 2024].

purposes of maintaining order and security on the occasion of events and demonstrations that gather large numbers of people. The mechanism automatically compares the face of a subject on the public road where it is installed with images stored in the data banks of the Central Identity Archive of the Home Office. The algorithm detects matches, the result of which is represented in a list of faces similar to the person being searched for, ordered according to a score indicating the degree of similarity[301]. The country's Guarantor for Data Protection has already ruled on the legality of this system when it acts in real time.

Thus, in the opinion issued on March 25, 2021, it establishes the way in which this mechanism acts, which is able to discover a correspondence between the face recorded by the camera and another present in the list, generating an alert to call the attention of the operators. The system records the video streams from the video cameras, which is why it performs surveillance activity. In addition, it performs a large-scale automated processing of those present at political and social demonstrations that are not the object of attention of the LEAs, which is why it suggests that there has been an evolution from the nature of this activity initially aimed at some subjects, to the possibility of universal surveillance in order to identify specific individuals. After assessing the impact of this system on various regulatory provisions, it considers that its use is inadmissible since we are dealing with a new biometric data processing that is not provided for in the current regulations. Therefore, its use raises some critical issues, at least in terms of the adoption of an adequate regulatory provision that disciplines its use for investigative or procedural purposes. Not only is the lack of *ad hoc* regulations the argument for which the Guarantor has prohibited its use, but it also understands that its implementation should be guaranteed only when strictly necessary and proportionate to its purposes, observing in any case the fundamental guarantees[302]. We will go into this aspect in more detail later in the corresponding section, but we bring it up at this point because it is a relevant example in the EU countries.

In Spain, since August 2023, even before the AIA was approved, the National Police has been using a FR tool called ABIS (automatic biometric identification system) in several cities such as Madrid, Barcelona, Granada, Malaga, Seville, Valencia and Valladolid. In addition, the National Guard also has FRs in two locations in the Spanish capital. The characteristic of this instrument is that image processing and identification are not performed in real time, but in delayed mode[303]. It will be necessary to wait for the

[301] TORRE, M. "Nuove tecnologie e trattamento dei dati boimetrici nel proceso penale: il sistema automatico di riconoscimento delle imagini", in Adinolfi, A. and Simoncini, A. (Dirs.), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizione Scientifiche Italiane, Napoli, 2022, p. 682.

[302] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, March 25, 2021 [9575877].

[303] PASCUAL, M.G. "La policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial", *El País*, 28 May 2024. Electronic resource obtained through the Web: https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html, [retrieved 10 Aug 2024]. The mechanism has been developed by the French military technology company Thales. It works by matching the image entered by the agents, taken from a security camera or a cell phone, with the photographs available in the system to look for

Spanish Data Protection Agency to make a decision on how it fits into the legal framework. However, a survey was made to the Head of the Identification Area of the Scientific Police Group of Granada, in which she explained and detailed how the system is used in Spain. This will be discussed below in the next section, as an example of the implementation of such mechanisms in the public sphere by LEAs for police investigation purposes.

In relation to the above, there are two types of RBIS used for law enforcement purposes, according to the AIA, those that act in delayed and those that act in real time. Nothing is said about the former, which are considered as a high-risk technique, while, on the contrary, the latter are prohibited in principle, with certain exceptions, as they are considered to seriously infringe the rights and freedoms of citizens. We understand that this provision may favour the extension of its use to other purposes, arguing the arguments of urgency and necessity in situations that would not require it. Therefore, in the following, we will address the regulation that the AIA makes of them, establishing the distinction between them as well as the guarantees and requirements that must be observed for a proper use.

III. REGULATION OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS IN THE AI ACT

1. Previous approaches to the AIA

The AIA is a pioneering regulation, as there is currently no other regulation addressing artificial intelligence in the public sphere, not even in the United States or China, where it has been used for some time[304]. The main objectives of the Regulation

matches. The database against which they are compared is made up of 4.4 million detainee profiles (3.2 from the National Police and 1.2 from the Civil Guard). Not only the image of the face is stored in this repository, but also the DNA and it is not connected with other European databases but, police agents assure, it will be. The comparisons made are one-to-one or one-to-many depending on whether they have the image of the suspect or not. The problem in our view is that it is not limited to serious crime, as originally envisaged, but is deployed for the prevention, investigation and detection of criminal offenses, as well as the protection and prevention of threats to public safety. As can be seen from the article, there are already sceptical voices about the inclusion of this technique in Spain.

[304] Although, as we have said, the AIA is the first public regulation on the subject, countries such as China and the United States have published texts containing some of the basic principles of AI. Thus, in 2019, the former promulgated the *Beijing AI Principles* of the Beijing Academy of Artificial Intelligence. In the same year, the *Principles to Develop Responsible AI for the New Generation Artificial Intelligence: Developing Responsible Artificial Intelligence* and, more recently, in 2023, *Interim Measures for the Administration of Generative Artificial Intelligence Services* were promulgated.

The G7 in October 2023 published two documents on IA principles: *Hiroshima Process International Code of Conduct for Organizations Developing advanced AI Systems* and *Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI system.*

In the United States, President Biden asked the seven major producers, such as Amazon, Anthropic, Google, Inflection, Meta, Microsoft and OpenAI, to develop some general standards. These

are to guarantee the development of AI while safeguarding a level playing field among operators in the internal market, while ensuring a high standard of rights protection[305], through a risk-based approach to rights. Thus, it is intended to fill the regulatory gap highlighted, among others, by the European Commission in the *White Paper*[306] and to achieve reliable AIs that operate on the basis of respect for the aforementioned rights[307]. Therefore, it has an anthropocentric approach as it aims to ensure human vigilance and the protection of the rights and freedoms of individuals against the risks arising from the use of such systems[308]. It also aims to establish an appropriate balance between economic development and the protection of rights[309].

In addition to the above, the other main purpose of the Regulation is to improve the functioning of the EU internal market through a uniform legal framework that establishes the conditions for developing the placing on the market, putting into service and use of AIs within the framework of the Union, in accordance with its values. Therefore, the legal basis of the Regulation is to be found in Art. 114 TFEU on the internal market. In this sense, the aim is to ensure a high and consistent level of protection in the Union to achieve a reliable AI, as well as to avoid divergences that hinder the free movement, innovation, deployment and adoption in the internal market of intelligent mechanisms and related products and services, through the establishment of uniform obligations for operators and ensuring an equally uniform protection of the general interest and the rights of individuals in the internal market.

Therefore, the implementation of these mechanisms must be human-centred and reliable, with an approach based on the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (hereinafter referred to as the Charter). Thus,

---

companies have committed to ensure the safe, reliable and transparent development of AI according to the fundamental principles of security and trust. The second is achieved by informing society of the content generated by the systems and specifying their limits.

The European vision of AI is based on an anthropocentric, ethical and sustainable approach and respectful of values and fundamental rights, as drawn from the *White Paper on Artificial Intelligence.* On the international texts based on AI principles that have been promulgated, see FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?...*, cit., pp. 45-47 and more extensively, at pp. 107-111.

[305] SCHEPISI, C. "Diritti fondamentali, principi democratici e *rule of law*: quale ruolo e quale responsabilità per gli stati nella regolazione dell'intelligenza artificiale", in Pajno, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, p. 204.

[306] EUROPEAN COMISSION, *White Paper...*, cit., p. 12.

[307] The AIA therefore regulates specific AIs or applications and not AI as a whole. This is seen, for example, in the classification of high-risk mechanisms and the establishment of specific rules for them. FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?...*, cit., p. 43. The author points out that it is one thing to regulate AI, but quite another to regulate its applications.

[308] DONATI, F. "Diritti fonamentali e algoritmi nella proposta di Regolamento sull'Intelligenza Artificial", in Pajno, A. et al. (Dirs.), *Intelligenza Artificiale e diritto: una rivoluzione?*, il Mulino, Bologna, 2022, p. 123.

[309] More specifically, with a human rights-based approach, the *Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, dated September 5, 2024, was signed in Vilnius on September 5, 2024, being perfectly compatible with the AIA, as it includes key concepts of the same. Its main purpose is to establish a common approach to ensure that activities carried out throughout the life cycle of AIs are compatible with human rights, democracy and the rule of law. It is a general document that does not classify the different IA mechanisms as the AIA does.

on the one hand, it aims to establish an uniform legal framework in the context of the Union on the use and development of AI mechanisms and, on the other hand, respect for the fundamental rights on which any mechanism to be implemented must be based. Thus, the Regulation is also based on art. 16 TFEU, since it contains specific rules to protect individuals with regard to the processing of personal data that restrict the use of AI when they are used for different purposes such as law enforcement, the performance of risk assessments of natural persons for purposes related to these objectives and for biometric categorization. In addition, the values of human dignity, democracy, equality, the rule of law and respect for human rights, including those of minorities, must be safeguarded in accordance with art. 2 TEU, as well as art. 6 TEU, which stipulates respect for the rights set forth in the Charter. This is because smart mechanisms have many benefits in many different areas but, at the same time, they also entail risks to public interests and fundamental rights.

As we have just noted, AI mechanisms offer many opportunities and benefits in different areas, including the exercise and protection of fundamental rights, but also entail some important risks. For this reason, it cannot be seen only as a threat but as an instrument that helps to improve the lives of individuals[310]. It seems that we are moving towards a new form of rights protection in this new digitalized society, of which we must be fully aware. The AIA is based on this philosophy, since the Commission starts from the idea that the new intelligent systems are the key to the economic and social development of the Union, and that their implementation must be combined with adequate regulation so that they do not represent a risk to the rights of individuals, but rather an instrument at their service.

In order to ensure that the rules are effective and proportionate, the AIA establishes a clearly defined risk-based approach that adapts the type of rules and their content to the intensity and scope of the hazards involved in the systems. It prohibits certain instruments as being unacceptably risky and considers other high-risk practices, for which it establishes strict discipline by setting specific requirements for their use and the obligations to be taken into account by operators, as well as the imposition of transparency requirements. On the other hand, limited risk systems only have to follow signalling obligations to warn users that they are interacting with an AIs, while minimum risk mechanisms, which include automatic translation services, have no restrictions[311].

[310] DONATI, F. "Diritti fonamentali e algoritmi nella proposta di Regolamento sull'Intelligenza Artificial...", cit. p. 114.

[311] This classification of systems according to the risk to the fundamental rights and freedoms of individuals is considered adequate by part of the doctrine. Among those in favour of it, *Ibd.*, p. 119, since it is considered suitable for balancing the need to protect rights with the need to promote the development of technological innovation. Nevertheless, the author points out that possible interpretative and application problems cannot be underestimated. The AIA is based on an identification of the degree of risk of the systems in the abstract and in a preventive way, which could in some cases prove to be inadequate in concrete cases.

RBIS are considered high risk[312] due to the danger they present in relation to citizens' rights and freedoms. Not only these are classified as such, but also those intended for other issues such as biometric categorization. Moreover, the AIA goes so far as to prohibit the use of RBIS that act in real time when used for law enforcement purposes in public places, considering that they represent an intolerable intrusion on the aforementioned rights except in certain cases, in which their use is permitted provided that certain requirements are observed. We will now describe the way in which the Regulation provides for such mechanisms, focusing on those used by LEAs in publicly accessible spaces (both those acting in real time and delayed), since they are the ones that generate most controversy, especially regarding the use of FRs.

2. Classification of RBIS with law enforcement purposes in public places

As already highlighted in Chapter I of this research, biometric identification refers to the automated recognition of physical, physiological or behavioural human characteristics to determine the identity of a person by comparing their biometric data with those of other individuals stored in a database, regardless of whether or not the person has given their consent. One of the most popular but no less controversial uses is facial recognition technology applied to video surveillance systems that allows the detection and unique identification of a person using his or her facial image. The latter is a parameter widely used in remote biometric identification but it is not the only one, since it can also be done through body movement or voice, among others. As previously stated on several occasions, our research focuses on FRs, not only because they are the most commonly used but also because they are of great concern, especially when they are implanted in public places for law enforcement purposes. The face is the element that identifies people par excellence and its indiscriminate use for identity determination purposes can have a serious impact on the rights and, therefore, on the living conditions of citizens.

In order to prevent this from happening, the AIA, through a risk-based approach, regulates the use of RBIS. As such mechanisms act with biometric and therefore personal data, the previous legal framework was the GDPR and the LED. The former provides the legal basis for the processing of personal data in general, excluding that carried out by competent authorities for the prevention, investigation, detection or prosecution of criminal offenses, or the enforcement thereof, including the protection against and prevention of threats to public security, as stated in art. 2.2 d) GDPR. For that reason, the

[312] The regulatory mechanism established for high-risk systems is not intended to prevent any violation of fundamental rights, but to limit the possibility of such a violation occurring. So that, through requirements, certifications and controls, it should be reduced to a level considered acceptable. ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro nomativo dell'Unione", in Pajno, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 157-158.

LED is designed as *lex specialis* with respect to the former in this context, being very similar its rules on data protection. Today, the regulatory framework of reference –at least as far as the FRs acting in real time are concerned– is the AIA, which proposes additional rules to the previous ones. However, for what is not covered by it (as we will have the opportunity to explain later), the former are still valid.

The AIA, especially with regard to our object of study, has been very controversial. Thus, once the initial proposal saw the light of day in April 2021, it was criticized for its treatment of RBIS in public places for law enforcement purposes[313]. As a result, various international institutions and organizations considered the need for a moratorium on its use. Among others, the United Nations High Commissioner of Human Rights on the Report *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies, including peaceful protests*[314]. In addition, the European Data Protection Supervisor (hereinafter EDPS) requested it from the Commission but the Commission did not take it into account[315].

Not only that, but it, together with the European Data Protection Board (EDPB) went further and demanded a general ban on any use of AI for these purposes[316]. Also the

[313] See, more extensively, CHRISTAKIS, T., BECUYWE, M., & AI-REGULATION TEAM. *Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021*, AI-Regulation.com, May 27th, 2021. Electronic resource obtained via the Web: https://ai-regulation.com/facial-recognition-inthe-draft-european-ai-regulation-final-report-on-thehigh-level-workshop-held-on-april-26-2021/, [retrieved May 7, 2024], pp. 1-16.

[314] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies, including peaceful protests*, 2020. A/HRC/44/24, p. 14. Moreover, it calls on law enforcement to refrain from using FR technology to identify those attending a peaceful assembly.

[315] EUROPEAN DATA PROTECTION SUPERVISOR. *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*. Retrieved from the World Wide Web: https://www.edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en, [retrieved May 8, 2024]. For that reason, he laments. He goes on to point out the need to establish a strict approach to the deployment of these techniques, as they can carry a high risk of intrusion into the privacy of individuals.

[316] EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 June 2021. Electronic resource obtained through the Web: https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf, [retrieved May 8, 2024], pp. 11-12. They also recommend that its use be prohibited in virtual spaces, as well as that of systems for categorizing individuals through biometrics.

Furthermore, within the Council of Europe, the AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE (CAHAI) recommended a partial moratorium or ban on AIs deemed to be of unacceptable risk, including biometric identification-based mechanisms, especially if they run the risk of mass surveillance. See the document *Possible elements of a legal framework on Artificial Intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law*, Strasbourg, 3 December 2021. CAHAI(2021)09rev, p. 5. However, it goes on to point out that such a moratorium or ban should only be considered when such a risk has been identified and, after careful examination, there is no other measure available that is less dangerous and just as efficient. Similarly, it concludes that review procedures should be established to allow a ban or moratorium to be revoked if the risks are sufficiently reduced and if there are adequate mitigation measures, on an objective basis, to no longer represent an unacceptable risk. The situation just noted is of concern to MANTELERO/FANUCCI, for whom this caveat may frustrate the purpose of banning or establishing exceptional moratoria on some AIs, since it is not clear how unacceptable risk systems can have possible legitimate exceptions when the impact on human rights is intolerable. MANTELERO, A. & FANUCCI, F. "The international debate on AI reputation and human

European Parliament in its Resolution of 6 October 2021 on *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, made this clear in nº. 27, establishing as exceptions the strict necessity of its deployment for the identification of crime victims, until the technical standards are considered fully in line with fundamental rights, the results are unbiased and non-discriminatory, the legal framework provides for strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence on the necessity and proportionality of its deployment[317]. Similarly, nº. 25 stipulates that this technology must at least meet the requirements of data minimization and accuracy, storage limitation, data security and accountability, in addition to having a lawful, fair and transparent use and pursuing a specific, explicit and legitimate purpose clearly defined in the legislation of the Member States or the Union. Thus, there is a duty to restrict its implementation to clearly justified purposes and to do so in full compliance with the applicable legislation as well as the principles of proportionality and necessity.

At the state level, specifically in Italy, Legge 3 dicembre 2021, nº. 205, in its point 9 established the suspension of the use of biometric data in public places or places open to the public, by the public authority or private subjects, until the entry into force of a legislative discipline expressly providing for it.

This legislative discipline has been materialized in the AIA, which after the various reforms it underwent (especially in this matter) was finally enacted on June 13, 2024. It aims to establish a functional concept of RIBS, located in art. 3.41), in which it defines it as "an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database". In addition, recital 17 states that these systems are often used to detect several persons or their behaviour simultaneously, with the aim of considerably simplifying identification without the active involvement of individuals.

From the above, some relevant elements that characterize RBIS can be extracted. Firstly, we are dealing with an AI whose purpose is the identification of natural persons "without their active participation, generally at a distance". This identification is carried

rights in the prism of the Council of Europe's CAHAI. Great ambitions", in Czech, P. et al. (Eds.), *European Yearbook on Human Rights 2022*, Intersentia, Cambridge, 2022, p. 247.

[317] Nº. 28 expresses serious concern about the use by law enforcement and police forces of private facial recognition databases such as Clearview AI and equivalent databases, as this would not be compatible with the Union's data protection regime. The Commission is asked to prohibit the use of private databases in the area of law enforcement.

In the same line are some authors who call for the total prohibition of FRs in criminal matters, both those acting in real time and those acting in deferred time. Thus, for example, WACHTER, S. "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What this means for the European Union, the United States, and beyond", *Yale Journal of Law & Technology, Special Issue: Yale Information Society Project Digital Public Sphere Series*, vol. 26, nº. 3, 2024, pp. 680, 716. Along with the above, he believes that emotion detection mechanisms should also be prohibited, especially in the field of immigration and criminal justice, as well as predictive policing tools.

out by comparing the biometric data of those individuals with those contained in a reference database, in which there is information on a multitude of individuals. In addition, RBIS are normally used to detect several people simultaneously, significantly simplifying this process.

As also indicated in the aforementioned recital, the AIA only provides for identification-oriented systems, which is why verification systems[318] are excluded, given that –as already stated– the sole purpose of the latter is to verify that a person is who he or she claims to be, as well as the identity of a natural person for the exclusive purpose of accessing a service or place and unlocking a device. This exclusion is justified by the lesser impact that such mechanisms have on the fundamental rights of citizens.

The Regulation classifies RBIS according to the time it takes to perform the identification. Thus, it distinguishes between "real time" and "delayed" systems. Both types of mechanisms are distinguished by the different intensity of their interference with fundamental rights. The former, as will be seen in the following, is prohibited except in specific exceptions. In such a case, it will be considered high-risk, together with the second. Thus, each one has different implications on the aforementioned rights, which is why they are treated differently in terms of their regulation, as will be explained immediately.

2.1. Remote biometric identification systems on real time

This type of mechanism, according to art. 3.42) AIA is defined as "a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention". As can be seen from the above definition, the process time is very short. For that reason, the materials used are "live" or "near-live" such as video recordings from a camera or other device with similar functions.

Given the short time lapse in the identification carried out by such systems, it is considered that they entail an excessive risk to fundamental rights and citizen guarantees. It should be taken into account that all RBIS are considered high risk by point 1 letter a) of Annex III of the Regulation. However, in view of the above, greater restrictions are imposed on their use when they are deployed in publicly accessible places for law

[318] Number 25 of the European Parliament Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). (2022/C 132/02), next to the use of verification/authentication of FRs differentiates between identification and detection. By the former he means the matching search of a photo with a database, while the latter he identifies as the detection of faces in real time from sources such as CCTV images and their matching with databases, e.g. real-time surveillance. This is what real-time RBIS would be.

enforcement purposes, to the extent of being prohibited in art. 5.1 h) AIA, with certain exceptions that will be detailed below.

2.1.1. Specification of the elements that constitute the prohibition of RBIS in real time in public access spaces with law enforcement purposes

At this point we define the two essential elements on which the regulation of RIBS is based in the AIA, common to both delayed and real-time systems. Therefore, although the analysis is carried out in this section, all the above is also transferred to the former.

A. Publicly accessible space

As the Regulation expressly regulates RBIS when they are used in public places, it is necessary to specify what is meant by them. As established in art. 3.44) AIA, public place is any physical space, regardless of whether it is privately or publicly owned, to which an undetermined number of natural persons may have access, and there may even be conditions for access and capacity restrictions. Recital 19 lists a series of activities that can be carried out in such spaces, which are very varied: commercial (stores, restaurants, cafeterias), provision of services (banks, professional activities, hotel and catering), sports (swimming pools, gymnasiums, stadiums), transportation (bus, metro and railroad stations, airports, means of transport), entertainment (cinemas, theatres, museums, concert halls, conference halls), leisure or otherwise (public roads and squares, parks, forests, playgrounds)[319]. Access may be subject to certain predefined capacity or security conditions and restrictions that may be met by an indeterminate number of people, such as the purchase of a ticket or a transport ticket, prior registration or being of a certain age. What is essential in this case is that the place is capable of accommodating an undefined number of people. In this sense, on the contrary, a space should not be considered publicly accessible if only certain defined natural persons may enter, either by virtue of Union law or national law directly related to public safety or by a clear manifestation of the will of the person exercising the relevant authority in that space.

[319] Similarly, the Venice Commission considers a public area to be any place accessible in principle to everyone freely, indiscriminately at any time and under any circumstances. So it is open to the public and everyone can have access. These areas are governed by public authorities, whose power to enforce the law and intervene is broader than in private property. By the latter he means any place whose access can be restricted by law and by those to whom it belongs. It is not open to the public in principle, it is not accessible to anyone, at any time and under any circumstances. It may happen that video surveillance systems and, by extension, FRs are deployed in such a way that they accidentally cover private spaces, which would constitute a visual intrusion by the authorities into people's homes. VENICE COMMISSION, *Opinion on video surveillance in public places by public authorities and the protection of human rights.* Study nº. 404/2006, Adopted at its 70th[th] Plenary Session (Venice, 16-17 March 2007). CDL-AD(2007)014, p. 4.

The fact that an environment is accessible, for example, when the door is unlocked or has an open gate, does not imply that it is publicly accessible if there are indications or circumstances that suggest otherwise, as is the case with signs prohibiting or restricting access. Premises owned by companies and factories, as well as offices and workplaces accessible only to employees and service providers are not public. Prisons and areas where border inspections are carried out are also not considered public access areas.

Certain areas may consist of both non-publicly accessible areas and publicly accessible areas. This is the case with airports or the lobby of a private residential building through which one enters a doctor's office. Online spaces are not public access places either, since they are not physical. However, whether or not a space is publicly accessible must be determined on a case-by-case basis, taking into account the particularities of the specific situation.

Although public spaces, as can be seen from the above, can be certain infrastructures such as airports, sports stadiums and other facilities capable of bringing together a large number of people, our study focuses on their application in uncontrolled spaces such as streets and similar environments as squares, where there is freedom of movement of individuals, where a large number of people can gather and where demonstrations and public protests can be held. Our research is confined to such environments because we consider them to be different scenarios. In the former, controlled environments, identification is usually carried out under appropriate lighting conditions. On the other hand, in uncontrolled environments such as the latter, where the images are exposed to changes in the conditions in which they are taken and are usually made in real time through video surveillance and CCTV systems[320], to which is added that the identification is made to an undetermined number of people who are unaware of or hostile to this form of surveillance[321]. Therefore, the installation in uncontrolled environments such as those mentioned above is capable of restricting or further limiting the rights and freedoms of citizens, especially in terms of freedom of movement, association, assembly and demonstration.

B. Law enforcement authority

The individuals entrusted with the task of implementing them are the LEAs. Art. 3.45) of the Regulation establishes the two forms that these authorities may take. On the one hand, at the individual level and, on the other, at the institutional level. Thus, they can be all those persons and institutions competent for the prevention, investigation, detection or prosecution of criminal offenses or the enforcement thereof, including the

[320] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe: a Non-Orwellian Draft Proposal", *European Journal on Criminal Policy and Research*, vol. 29, nº. 4, 2021, p. 528.

[321] MOBILIO, G. "Your face is not new for me...", cit., p. 5.

protection and prevention of threats to public safety. Art. 1.1 LED, with a more restricted approach, only mentions the latter.

Finally, law enforcement, as stated in art. 3.46) AIA, would be all those "activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security".

The European Parliament and the Council are aware of the risks involved in these systems. For this reason, in recital 32 AIA they state that they entail a particularly serious encroachment on the rights and freedoms of individuals, insofar as they may affect the privacy of a large part of the population, give rise to a feeling of constant surveillance and indirectly dissuade society from exercising its fundamental rights, including freedom of assembly. On the other hand, they warn, not only in this recital, but also in recital 54, about the technical inaccuracies of these mechanisms, which can lead to biased results and have a discriminatory effect, especially in relation to age, ethnicity, race, sex or disability. In addition, the immediacy of the consequences and the reduced opportunities for checks or corrections further increase the risk to the rights and freedoms of those affected.

2.1.2. Exceptions to the ban of use of real-time mechanisms stablished in the art. 5.1.h) AIA

For the reasons stated above and, given that real-time RIBS in publicly accessible places for law enforcement purposes entails a virtually immediate automated decision that can severely affect rights and freedoms, the AIA in its art. 5.1 letter h) included in Chapter II on prohibited AI practices, vetoes its use. However, it lists and precisely defines three situations in which it may be used provided that it is necessary to achieve an essential public interest whose importance outweighs the risks. These situations are:

a) Selective search for victims of a crime of kidnapping, human trafficking or sexual exploitation, as well as the search for missing persons;
b) Prevention of specific, significant and imminent threats to the life or physical safety of natural persons or actual and present or actual and foreseeable threats of terrorist attack;
c) Location or identification of perpetrators or suspects of having committed an offense for the purpose of criminal investigation or prosecution or execution of such a sanction for any of the offenses provided for in Annex II of the Regulation, when the same are punishable by a custodial sentence or security measure with a maximum duration of at least four years. As a justification for the use of such instruments in this specific case, the contribution to ensure that the offense is sufficiently serious to legitimize the use of these RBIS is established. In addition, these criminal offenses are based on the thirty-two

> offenses listed in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (DO L 190 of 18 July 2002). Such offenses are the following: a. Terrorism; b. Human trafficking; c. Sexual exploitation of minors and child pornography; d. Illicit trafficking in narcotic drugs or psychotropic substances; e. Trafficking in arms, ammunition and explosives; f. Voluntary manslaughter, assault and battery with serious injury; g. Illicit trafficking of human organs or tissues; h. Illicit trafficking of nuclear or radioactive materials; i. Kidnapping, illegal detention or hostage-taking; j. Crimes under the jurisdiction of the International Criminal Court; k. Hijacking of aircrafts or vessels; l. Rape; m. Crimes against the environment; n. Organized or armed robbery; ñ. Sabotage; o. Participation in a criminal organization involved in one or more of the crimes enumerated in this list.

Notwithstanding this, as highlighted in recital 33, in practice, some infringements are more relevant than others, making it necessary and proportionate in some cases to resort to these systems. Similarly, there are likely to be differences in the seriousness, likelihood and magnitude of the prejudice or possible negative consequences. This issue is criticized by part of the doctrine, which considers that the list of offenses in which this system can be used is not so restrictive, since some crimes are not serious enough to legitimize its use, given that they do not affect the life of persons or their physical integrity[322]. Thus, together with the limitation by the type of crime committed, they believe that it would be interesting to include as an additional restriction the type of individuals who can be subject to identification, limiting it to those who are particularly suspicious to the police[323]. This would further limit the use of RBIS. Despite of the above, the question arises as to the difficulty posed by this limitation, since in uncontrolled environments, the video surveillance system would record the images of all faces, with all individuals passing through a given place being exposed to identification.

Regarding what is to be understood as an imminent threat to the life or security of natural persons, following the provisions of the aforementioned recital, they would be those that come not only from the aforementioned crimes but may also derive from a serious disruption of critical infrastructures, being these an element, facility, equipment, network or system, or part of an element, facility, equipment, network or system, which is necessary for the provision of an essential service[324]. The disruption or destruction of such infrastructure must pose an imminent threat to the life or physical safety of a person,

[322] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 522.

[323] *Idem*. The author goes on to point out that this should be the case, unless the circumstances of the criminal investigation require a broader objective, duly justified in each situation by the competent authorities.

[324] Article 2.4) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

especially by seriously impairing the supply of commodities or the exercise of the essential function of the State.

In addition, the AIA is intended to preserve the ability of LEAs, border control, immigration or asylum authorities to carry out identity checks on the individuals concerned. The authorities entrusted with these functions may use information systems, in accordance with EU or national law, to identify subjects who, during an identity check, refuse to be identified or are unable to declare or prove their identity, without the need for prior authorization to do so (for example, a person involved in a crime who does not want to reveal his identity or is unable to do so due to an accident or medical condition).

These systems are not automatically applied in the cases indicated to confirm the identity of the person who constitutes the specific target, but, by virtue of what is established in recital 34, their scope of application is limited to the confirmation of the identity of the subject who constitutes the target and limited to the period of time and geographical and personal scope strictly necessary. In addition, certain elements must be considered when any of the three situations indicated occur and must always be done in a responsible and proportionate manner.

These elements are included in the second paragraph of art. 5 AIA and are based on the seriousness and probability of the risk situation occurring and the damage that could be caused to the rights and freedoms of those affected. Thus, it literally establishes that the assessment will take into account: "a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used; b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences".

In addition to the above, the necessary and proportionate guarantees and conditions must be met in relation to time, geographic and person-related limitations, considering the evidence or indications regarding threats, victims or perpetrators. On the other hand, prior to the implementation of the system, an assessment of the impact on fundamental rights must be carried out by the law enforcement authority (as provided for in art. 27 AIA[325]) and registered in the appropriate EU database in accordance with art. 49 AIA.

[325] The evaluation according to the first paragraph of the aforementioned precept shall consist of:

"(a) description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;

b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;

c) the categories of natural persons and groups likely to be affected by its use in the specific context;

d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to article 13;

Not only must the above requirements be met for an RBIS of the characteristics analyzed in this section to be implemented, but it is also subject to the granting of prior authorization from an independent judicial or administrative authority whose decision is binding on the Member State where the system is to be deployed (Art. 5.3 AIA). This authority has the power to refuse authorization as it must only grant it when it is satisfied that the use of the system is necessary and proportionate to achieve one of the objectives set out in the exceptions to use. It will be granted upon a reasoned request and in accordance with the rules of national law set out in paragraph 5, i.e. the implementation of these mechanisms is limited to the extent that the particular Member State decides to expressly provide for this possibility in the rules of its national law and to the extent that it has done so. Thus, countries are free to provide or not to provide for this option or to offer it for certain purposes that may justify an authorized use as established in the Regulation. Therefore, each country has the power to specify the necessary rules applicable to the application, granting and exercise of the authorizations, as well as to the supervision and notification thereof.

Such rules shall specify the purposes for which it is implemented and in relation to the specific offenses listed above. However, in duly justified cases of urgency, this provision will not be necessary, provided that the search is subsequently carried out without undue delay, i.e. within 24 hours at the latest. It may happen in this case that the authorization is rejected, so that the use of the system must be immediately interrupted and all related data, as well as the results and output information created, discarded and deleted. A very important issue that ends the third paragraph is the prohibition that decisions leading to adverse legal effects for a person are taken exclusively on the basis of RBIS output information.

This immediately follows the provisions of art. 11 LED, which prohibits automated decision making, meaning any decision based solely on automatic data processing, including profiling that produces legal effects on an individual or significantly affects him. Moreover, an automatic arrest cannot be derived from it, since in any case the decisions issued by the mechanism must be confirmed by a human operator. There are exceptions to this prohibition provided that there are circumstances that are expressly

e) a description of the implementation of human oversight measures, according to the instructions for use;

f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms".

As stated in paragraph two of the same, the above obligation applies to the first use of the system but the deployer may rely on previous or existing fundamental rights impact assessments carried out by suppliers. If during the use of the system the deployer considers that any of the elements in paragraph one have changed or are not up to date, he or she will deploy the appropriate measures to update the information. Once the impact assessment has been carried out, section three details that the deployer will notify the market surveillance authority of the results. In the event that the obligations set out in this precept are already fulfilled as a result of an impact assessment carried out under art. 35 GDPR or 27 LED, the assessment referred to in this paragraph will complement those (paragraph 4). Finally, the AI Office will make a model questionnaire through an automated tool to facilitate those responsible for the deployment to comply with their obligations in a simplified way.

provided for by law and that offer adequate safeguards for the rights and freedoms of the individuals involved. As explicitly stated in the aforementioned precept, such exceptions apply only when strictly necessary and based on solid arguments.

Without prejudice to the above, the use of the mechanisms shall be notified to the relevant market surveillance and national data protection authority following the specific rules established by each Member State (Art. 5.4 AIA). These authorities must submit annual reports on the use of the mechanism to the Commission. For this purpose, the Commission shall provide the Member States and national market surveillance and data protection authorities with a model including information on the number of decisions taken by the competent national or independent administrative authority whose decision is binding (Art. 5.6 AIA). Paragraph 7 of the same provision stipulates that the Commission must publish annual reports on the use of the systems based on aggregated data relating to the Member States according to the annual reports, which shall not include sensitive operational data from related law enforcement activities. According to paragraph 8 of the above-mentioned article, this shall not affect the prohibitions applicable when an AI practice infringes another legislative act of the Union.

As the use of RBIS involves the processing of biometric data, the provisions of the Regulation, in the sense of prohibiting its use except for certain exceptions already mentioned, must be applied as *lex specialis* with respect to art. 10 LED, which also prohibits the use of biometrics unless it is strictly necessary, subject to adequate safeguards and authorized by the Member State in question. This comprehensively regulates the use and processing of biometric data when the system is used by a law enforcement authority in public places.

Thus, the use and processing of such data will be carried out only to the extent that it is compatible with the provisions of the Regulation, without there being any margin for the competent authorities, when acting for law enforcement purposes, to do so in compliance with the above requirements and only in the cases provided for in the Regulation. This is a novel issue for two reasons. Firstly, because the AIA aims to completely prohibit RBIS in real time except when it is to satisfy the three purposes provided for in the Regulation, it being understood that, in this way, the requirement of "strict necessity" provided for both in art. 10 LED and, specifically, in art. 5.2 AIA is met. Secondly, authorization by the appropriate judicial or administrative authority is required. This last provision was not previously included in any other document.

Therefore, in view of the serious consequences that may arise for fundamental rights and freedoms, its use is limited to the cases expressly contemplated in the AIA, provided that certain conditions are met and the circumstances make it advisable. The aim is to ensure a limited use. However, despite the exceptionality, we consider that in some scenarios the possibilities of application could be extended and exceeded, using the arguments of urgency and necessity, especially when prior authorization for the use has

not been requested, which entails a serious danger, since too much freedom is left to the LEAs to decide when to implement it.

These systems are particularly intrusive and severely interfere with the rights and freedoms of the individuals involved, affect the privacy of a large part of the population, can cause constant surveillance and indirectly deter the exercise of freedom of assembly and other fundamental rights protected under EU law. Moreover, their immediate action increases the risk of violation of the rights of individuals. In practice, the AIA is intended to prohibit the use of these mechanisms in public places when the intention is to deploy them in public demonstrations or to locate persons responsible for minor offenses[326]. For this reason, their use is censored except in the three scenarios described above, as long as all the necessary limits and guarantees are observed. Nevertheless, as we have said, the risk of its use extending to other areas that do not require it is high.

On the other hand, each Member State, as we have indicated, is entitled to decide whether to provide for all, only some or none of these in its domestic legislation. In this way, the AIA takes into account that security issues remain the exclusive competence of each country and tries to maintain a balance between security and public order on the one hand and, on the other hand, data protection and other fundamental rights that RBIS jeopardize. States do not have to establish a clause in their national regulations specifying the authorization to use such systems, they only have to adopt the exceptions in a clear and detailed manner.

As each country is entitled to introduce the regulations as it sees fit, there is a risk of fragmentation in the use of the systems between countries, due to different regulation depending on the State in question, especially with regard to the aspect of how to deal with necessity and proportionality[327]. Added to this is the problem of how to achieve a homogeneous level of consistency and coherence when interpreting the legal requirements imposed by the Regulation.

2.2. Delayed remote biometric identification systems

The above are the only RBIS whose use is prohibited while the others are classified as high risk, as they also interfere with rights and may have some technical shortcomings that could lead to biased results and discriminatory effects. They are therefore subject to stringent safeguards and must meet mandatory requirements to ensure that they do not entail unacceptable risks to essential public interests of the Union. Such

[326] CHRISTAKIS, T. BECUYWE, M. & AI-REGULATION TEAM. *Facial Recognition in the Draft European AI Regulation...*, cit., p. 5.

[327] In the opposite sense, DONATI, F. "Diritti fondamentali e algoritmi...", cit, p. 120. The author considers that the decision to adopt a Regulation and not a Directive is appropriate, since the Commission proposes an uniform discipline to prevent national regulations from fragmenting the internal market and diminishing the certainty of the law for operators developing or using AIs.

systems include real-time RIBS in publicly accessible places used by public authorities for purposes other than law enforcement, by private actors such as private security companies for any purpose and by any other actor (including LEAs) in spaces that are not publicly accessible; delayed RBIS extending also to those used in publicly accessible areas for law enforcement purposes and any use of FRs that does not fit the definition offered in the AIA, such as their use for authentication purposes in access security protocols, where the system is able to determine a one-to-one match to confirm that the person is who they claim to be[328]. As interesting as it may be to study the aspects concerning all of the above, we will focus on deferred RBIS for law enforcement purposes in public places, due to the particularities they present.

2.2.1. Delayed RBIS term

First of all, we must specify what is meant by such systems. If the previous ones involved an immediate identification or without excessive time delay, the deferred RBIS would be those in which the identification takes place over a longer period of time. Art. 4.43) AIA establishes a definition of these systems that does not help to clarify what this type of system is, specifying "a remote biometric identification system other than a real-time remote biometric identification system". As can be seen from the above, the Regulation does not include a specific term, thus leaving a vague and imprecise concept, subject to the provisions for real-time systems, more specifically, what is not understood by them.

Recital 17 helps to clarify the way in which these mechanisms operate, establishing that they do so with a significant delay between the collection of the data and the comparison and identification. The materials used are images or video recordings captured by CCTV or private devices, created prior to the use of the system in relation to the natural persons in question.

For the previous ones, the prohibition of their use established in article 5.1.h) AIA was applicable. However, this is not applicable to the ones now analysed, since it is understood that the intrusion in fundamental rights is not of the same magnitude as in the former. Despite this, they are considered high risk, given that Annex III 1 of the AIA qualifies biometrics in this way, insofar as their use is permitted by applicable Union or national law and, more specifically, letter a) includes remote biometric identification systems in general, so that they will have to observe the guarantees and requirements provided for in the AIA for high-risk systems. For this reason, the use of delayed RBIS is subject to the conditions set out in art. 10 LED, so the restriction is less than that established for the previous case.

[328] CHRISTAKIS, T., BECUYWE, M., & AI-REGULATION TEAM. *Facial Recognition in the Draft European AI Regulation...*, cit., p. 6.

Together with the systems now analysed, letter b) includes as high risk, AIs intended to be used for biometric categorization according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics, AIs for emotion recognition. This distinction, along with the general distinction between real-time and delayed systems, has been criticized as arbitrary, since biometric categorization mechanisms using multiple elements could allow identification to adversely affect fundamental rights in the same way as real-time RBIS. Added to this is the fact that most FRs act a posteriori and that the disparity of the limitations of biometric identification compared to categorization or emotion recognition does not take into account the harms that can arise from the latter[329].

2.2.2. Conditions of use according to the AIA and data protection regulations

Leaving aside biometric categorization in particular and, returning to delayed RBIS in publicly accessible places for law enforcement purposes, the conditions under which they can be used are set out in art. 26.10 AIA. Thus, the deployment of the system must be subject to safeguards due to its intrusive nature, without prejudice to the provisions of the GDPR and the LED. Thus, the mechanisms must always be used in a proportionate and legitimate manner, when strictly necessary and thus selectively in terms of persons to be identified, location and temporal scope and from a limited data set of video recordings obtained in a lawful manner. As can be seen, although there are conditions, they are not as demanding as the previous ones, but this should not serve as an excuse for LEAs to circumvent the conditions of the prohibition and the strict exceptions applicable to remote identification in real time, making use of delayed mechanisms in a way that is not in line with the provisions of the Regulation, which could lead to indiscriminate surveillance.

When an investigation is being conducted for the purpose of searching for a suspected or convicted criminal offender, the prior authorization requirement is maintained. In this case, the person responsible for deploying the system must request it in advance or without undue delay from the appropriate judicial or administrative authority within a maximum period of 48 hours, which is longer than in the previous case. This provision does not apply when it is used for the initial identification of a possible suspect on the basis of objective and verifiable facts directly linked to the offense. Each use must be limited to what is strictly necessary to investigate a specific criminal offense. In the event that authorization is denied, the system must cease to be used immediately and the associated personal data must be deleted.

[329] See, in this sense, KIND, C. "Containing the canary in the AI coalmine-the EU's efforts to regulate biometrics...", cit.

Be that as it may, delayed RBIS should not be used in law enforcement in a manner that produces indiscriminate surveillance (as noted above), i.e., unrelated to a criminal offense, a criminal prosecution, a real and present or real and foreseeable threat of a criminal offense, or to the search for a specific missing person. LEAs will be vigilant to ensure that they cannot make decisions that produce adverse legal effects based solely on the information provided by these systems.

This is without prejudice to the provisions of art. 9 GDPR and 10 LED. Both precepts prohibit the use of biometric data aimed at uniquely identifying a natural person except when there are a number of exceptions. The second paragraph of the first one, letter g) establishes as an exception to this prohibition the need when there is an essential public interest, which must be proportional to the objective pursued, essentially respect the right to data protection and establish adequate and specific measures to protect the interests and fundamental rights of the data subject. As it is developed in the field of criminal investigation, the normative framework of reference will be the LED, which refers in the indicated precept to issues of strict necessity and respect for the rights and freedoms of the data subject only when authorized by the law of the Union or Member State; it is necessary to protect the vital interests of the data subject or of another natural person; or the processing is of data that the data subject has manifestly made public.

Regardless of the purpose, any use of delayed RBIS shall be documented in the appropriate police file and made available, upon request, to the relevant market surveillance and the national data protection authorities, excluding the disclosure of sensitive operational data with the application of the Law. This is without prejudice to the powers conferred by the LED to the supervisory authorities in its art. 47:

1) Of investigation, which shall include at least the power to obtain from the controller and the processor access to all personal data being processed and to all information necessary for the performance of their duties.
2) Corrective measures, such as issuing warnings to controllers or processors when processing operations are likely to infringe the provisions adopted in the Directive, ordering them to bring processing operations into conformity with the provisions adopted pursuant to the Directive, in a certain manner and within a specific time limit, in particular by ordering the rectification or erasure of personal data, or the restriction of their processing and the imposition of temporary or definitive restrictions on processing, including the prohibition of processing.
3) Effective advisory powers to advise the controller in accordance with the prior consultation procedure and to deliver, on its own initiative or upon request, opinions addressed to the national Parliament and its Government or, in accordance with the law of the Member State, to other institutions and bodies,

as well as to the public, on any matter relating to the protection of personal data[330] .

Deployers are required to submit annual reports to the market surveillance authority and the national data protection authority on their use of delayed RBIS, excluding the disclosure of sensitive operational data linked to law enforcement. The reports may be aggregated to cover more than one deployment. Finally, the last paragraph of this section set the possibility for States to adopt, according to Union law, more restrictive laws on the use of these mechanisms.

Any processing of biometric data used for remote identification for law enforcement purposes other than in real time must comply, as we say, with the provisions of art. 10 LED and, when the use is authorized, must also respect the principles set forth in art. 4.1 LED, i.e. that the data must be processed lawfully and fairly; collected for specified, explicit and legitimate purposes, and not be processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are processed; accurate and, if necessary, kept up to date. All reasonable steps must be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay; kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which they are processed; and that the processing is carried out with appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, through the implementation of appropriate technical or organizational measures.

The distinction made by the AIA between this type of systems and the previous ones is made taking into account the different characteristics and forms of use they present as well as the different level of risk they entail. However, this is questionable because both are intrusive, given that the level of intrusion into rights and freedoms does not depend on the time of data processing. Moreover, the continued use of delayed intrusions can lead to a situation of mass surveillance.

RBIS can identify thousands of people in a few hours and, if used in a political protest for example, the use of remote systems will probably have a perverse effect on the exercise of rights and freedoms. So these are jeopardized in both modalities, not only in those mechanisms that act in real time[331], since those that perform the identification *a*

[330] The fourth paragraph of the aforementioned provision states that the powers conferred on the supervisory authority are subject to appropriate safeguards, including effective judicial protection and respect for the procedural guarantees established in Union and Member State law in accordance with the Charter; and the fifth, that each Member State shall provide by law that its supervisory authority is empowered to bring infringements of the Directive to the attention of the judicial authorities and to initiate or otherwise prosecute proceedings for the purpose of enforcing the provisions adopted pursuant to the Directive.

[331] EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence...*, cit., p. 13. Of this opinion also, MILOSSI, M. "Remote biometric identification systems and ethical challenges: The case of

posteriori have a similar negative impact on privacy, association and other fundamental rights.

In this way, we reiterate, there is a risk of provoking a more intrusive mass surveillance even when the data are processed from sources obtained at different times and places. The distinction is clearly artificial, because deferred use can lead to continuous monitoring of the individual's private life data[332]. It may even happen that in the field of political protests it may have a relevant dissuasive effect on the exercise of certain rights and freedoms and, in general, on the founding principles of democracy. Moreover, despite the limitations foreseen, the potential number of suspects or perpetrators of crimes will normally be so high as to justify the continued use of systems to identify them. For all these reasons, the EDPB and EDPS are against the implementation of automatic human trait recognition systems in public access places, even going so far as to call for their general prohibition, not only faces but also other parameters such as gait, fingerprints, DNA, voice and other biometric or behavioural signals, in any context[333].

In this regard, the ECHR *Case Glukhin v. Russia*, of October 4, 2023, where the Court considered that the right to privacy and freedom of expression provided for in articles 8 and 10 of the European Convention on Human Rights (hereinafter, the Convention) were violated, respectively, because the police had arrested an individual participating in a peaceful individual demonstration days after it had taken place by recording the place where it was held. This leads us to assert that both real-time and delayed RBIS entail excessive interference with fundamental rights and, for that reason, should be subject to the same restrictions.

With a similar approach, MURRAY considers that the time lag between the recording of the images and the retrospective application of the FR can be negligible, since the latter can be used to generate an alert capable of influencing the present, as occurred in the case just discussed. In addition, the operation of a real-time FR via CCTV and the application of the retrospective FR to the data recorded from the CCTVs entail a

facial recognition", *21st 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 2021, p. 5; BARKANE, I. "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance", *Information Polity*, nº. 27, 2022, p. 152; SCHRÖDER, A. "'Real-time' versus 'post'biometric identification systems under the AI Act", *ALTI Forum*, 14 October 2022. Electronic resource obtained via the Web: https://alti.amsterdam/schroder-biometric/, [retrieved 22 May 2024]. On this issue it is also worth noting that the European Parliament Research Service states that FRs entail a risk to fundamental rights, without distinguishing between those that act in real time or *a posteriori*: MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU*, p. 8; & MOBILIO, G. "Your face is not new to me...", cit., pp. 20-21.

[332] SCHRÖDER, A. "'Real-time' versus 'post'biometric identification systems under the AI Act...", cit.

[333] EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence...*, cit., p. 13.

similar level of surveillance and intrusion. In short, FR is used to identify who is present in a digital image, either in real time or delayed[334].

For this reason, we believe that the distinction made in the AIA is inadequate, since both types of systems interfere considerably with citizens' rights and can have severe consequences, including a scenario of mass surveillance. Thus, they should be subject to similar restrictions.

2.2.3. Case study: Implementation of a delayed face recognition system by the national police in Spain

In Spain, for some months now, the National Police has been implementing a FRs that acts in deferred mode in different cities of the Spanish territory. Thus, the pilot program began to be used in Madrid at the end of 2023 and, subsequently, reached some cities such as Granada, specifically at the beginning of March 2024. To find out how it works, a semi-structured interview was conducted with the Head of the Forensic Police identification area in this city.

After presenting the study and why it is important to have the information it can provide for our research, consent was requested to record the content of the conversation. Once this was obtained, we went on to ask the different questions of interest[335]. These were divided into three blocks: in the first, the aim was to find out the basis and way in which the systems operate; in the second, the impact of the technique on crime levels in order to find out its effectiveness; and finally, the third block includes questions on the impact on the rights and freedoms of citizens, as well as a personal assessment of the progress of technological means to combat crime.

The particularity of this mechanism is that it does not act immediately, i.e. it is not of the real-time type, but deferred. Therefore, it operates with the recordings resulting from a video-camera, after some time has elapsed since the commission of the criminal act in question and the materials do not correspond to the images of people passing through a certain place indiscriminately. In order for it to start working, the police unit investigating an incident, requests its implementation to the identification unit of the Scientific Police, who work with the recordings. Within the recordings, the individual to be identified is located.

The system does not offer absolute results, but makes a list of possible candidates that, according to a series of parameters, offers those that are most similar to the person to be identified, once the appropriate comparisons have been made with the databases. Once these similarity indexes are available, the role of the specialist police officer comes

[334] MURRAY, D. "Facial recognition and the end of human rights...", cit., pp. 147-148.
[335] The issues raised can be consulted in Annex I of this research.

into play, who will determine whether the candidate offered by the mechanism is the possible perpetrator or not. He will then decide whether to provide this information to the group in charge of the investigation or whether, on the contrary, no candidate should be offered.

For this reason, this is one more tool in the investigation process and does not lead to an arrest immediately after the result, but continues to investigate the case, in the sense of corroborating that the individual identified is the author of the facts and, if so, would proceed to arrest. As it is a novelty, there are no studies on its effectiveness, but the average is between seven and eight requests for use per month, that is, about fifty since it was launched in the city of Granada. At the beginning, as the technique was not very well known, there were not many requests but, from the moment it was observed that it produced good results, the number of requests increased. For this reason, the mechanism has been well received by crime investigation units.

With regard to the level of success, the rate is 50% and a greater impact is expected in the future. At present, being very new, like any technology in its infancy, it has some shortcomings that will be polished with the passage of time. In this sense, as the Chief Inspector affirms, it will be refined and will have more involvement as a surveillance tool. In addition to what has just been pointed out, there is the expansion of video surveillance systems in public places, which will allow its greater use in this environment, given that, if there are more devices of this type, it is easier to provide recordings.

Thus, in relation to the situations and crimes in which technology has been used, it is usually in public spaces that already have surveillance devices, as in the case of ATMs, not so much in the public (uncontrolled) space *per se*. Therefore, there is no risk that it could lead to a possible monitoring of the movements of individuals if it is only limited to those specific environments and spatio-temporally determined recordings based on individualized suspicion.

An issue of great interest, as we will have the opportunity to discuss later in the following chapter, is the question of the databases used for identification, insofar as the right to personal data protection may be violated if the databases are made up of images taken, for example, from social networks or created by private companies that sell them to the LEAs. In this specific case, only national police databases of wanted persons, suspects, etc., are used, so they are protocolized and unified at this level for the entire Spanish National Police Force. In this way, a specific Police Headquarters cannot resort to the databases it deems appropriate beyond those commonly established at the state level. Regarding social networks, it is confirmed that they are not used, unless required by the investigation and the image is provided by the victim himself. On the other hand, the images are stored for a reasonable period of time and are deleted every so often, also in a centralized manner.

With the current state of technology, its use limited to the cases and conditions indicated and, in view of the guarantees of a democratic country like Spain, it would be

impossible for the use of this FRs to result in a restriction of rights such as the right of movement. The Head of the Identification Unit alludes to a very interesting issue, such as the normality and everyday use of biometric techniques in actions such as unlocking the screen of Smartphones because, as will be observed in the last chapter of this research, this normality is what favours citizens not to perceive the dangers that technology can entail when used in the field of public safety.

However, it seems that we do not have to fear the implementation and extension of this mechanism in Spain, since its use is very limited and it has a series of guarantees and requirements. In spite of this, we cannot allow it to expand more than necessary and, if it produces good results, we can begin to justify its generalization and that it may even reach real-time systems. As we have already pointed out, we have to wait to see how the EU States will implement the AIA in the aspect concerning these systems. It is true that LEAs cannot lag behind and have to adapt to technological advances and use them to combat and control crime, since the latter already makes use of them. For this reason, in the opinion of the Chief Inspector of the Identification Area of the Scientific Police of Granada, due to the threats posed by crime today, more advanced, trained personnel with more resources are needed for what may come in the future. This does not prevent us from understanding the need for them to be subject to similar requirements and conditions as those established for the mechanisms that act in real time because their indiscriminate use is also likely to impact on the rights and freedoms of citizens.

3. Common aspects of high-risk AIs

As both delayed and real-time RBIS once their use has been authorized are qualified as high risk, their putting into service or use must be carried out in strict compliance with mandatory requirements common to all AIs with such qualification –independently of those specific to each one–, taking into account their intended purposes, the context of use of the instrument and the state of the art, as established in art. 8 AIA, and aimed at ensuring that such mechanisms do not entail unacceptable risks to important public interests of the EU. They must take into account in particular the state of the art, be proportionate and effective in achieving the objectives set out in the Regulation. Furthermore, the mechanisms must be in line with the risk management system envisaged by the supplier, as provided for in Art. 9 AIA[336].

[336] This risk management system, as stated in the second paragraph of art. 9 AIA, must consist of a continuous iterative process planned and executed during the entire life cycle of the high-risk AI, which will require periodic reviews and updates. The process should aim to identify and mitigate risks to health, safety and fundamental rights mechanisms. The system should be reviewed and updated on a regular basis to ensure its effectiveness, as well as the justification and documentation of significant decisions and actions taken based on the Regulation. The process must ensure that the supplier identifies risks or adverse effects and implements measures to mitigate those that are known and reasonably foreseeable to health, safety and

Thus, all RBIS have to observe a number of requirements prior to their commissioning and, along with risk management measures, must ensure transparency and provide users with adequate information, implement suitable human supervision measures and ensure that the mechanisms are designed with an adequate level of accuracy, robustness and safety. The systems must be subject to strict pre-commissioning conformity procedures that both suppliers and users must adhere to, as well as undergo conformity assessment by an independent body. Once the system has passed the above phases and has been placed on the market, it can be used by public or private actors (depending on the fields and purposes for which it has been developed, in our case, in public places for the purpose of law enforcement) in accordance with EU law. In particular, the provisions of the GDPR and, more specifically, the LED, which regulates the protection of personal data in the criminal field, must be complied with. In addition to the above, subsequent monitoring and supervision must be carried out.

As indicated above, RBIS entail a high risk to fundamental rights. Recital 48 lists the rights that may be endangered by the use of high-risk systems in general, including human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and association, non-discrimination, the right to education, consumer protection, workers' rights, the rights of persons with disabilities, equality of treatment, the right to privacy, the right to intellectual property, the right to effective judicial protection, and to an impartial judge, the rights of the defence and the presumption of innocence, and the right to good administration. In addition to the above, the specific rights of minors set out in art. 24 of the Charter and in the United Nations Convention on the Rights of the Child, developed more extensively in observation nº. 25 of the Committee on the Rights of the Child in the digital environment. The fundamental right to a high level of environmental protection is also added.

For its part, the *White Paper on Artificial Intelligence* lists the rights that are endangered by the specific use of RBIS in public places, being the following: personal dignity and, linked to this, the rights to respect for privacy and the protection of personal data, the right to non-discrimination and the rights of specific groups such as children, the elderly or people with disabilities. To the above are added the freedoms of expression, association and assembly[337]. The European Union Agency for Fundamental Rights (FRA) expands the list of rights that may be more affected by the use of facial recognition in the

fundamental rights. In addition, the system has to adopt appropriate risk management measures according to the current state of the art in AI.

Systems shall be tested to determine the most appropriate and specific risk management measures. These tests shall verify that the high-risk systems operate in a manner consistent with their intended purpose and meet the requirements and may be performed at any time prior to their introduction to the market or commissioning. They shall be performed using defined parameters and probability thresholds that are appropriate for the intended purpose of the high-risk AI.

The instructions for use provided by the supplier must include any known or foreseeable circumstances, linked to the use of the high-risk AIs, taking into account its intended purpose or reasonably foreseeable misuse, which may result in risks. This is to ensure that the commissioning manager is aware of such risks and considers them when using the system.

[337] EUROPEAN COMMISSION. *White Paper on Artificial Intelligence...*, cit. p. 26.

context of law enforcement in public places, adding the right to good administration, to an effective remedy[338].

The Parliament and the Council are aware of the serious consequences that can result from the actions of LEAs when using AIs. Thus, in recital 59 they state that it involves a significant imbalance of power and can lead to surveillance, detention or deprivation of freedom of a natural person and have negative effects on fundamental rights. When the system is not trained with good quality data[339], does not meet the appropriate requirements on performance, accuracy or robustness, or even if it is not properly designed and tested before being introduced into the market or put into service, it can lead to individuals being singled out in a discriminatory, incorrect or unfair manner. It could even have an impact on fundamental procedural rights, such as the presumption of innocence, effective judicial protection and the right to an impartial judge, especially when the mechanisms are not sufficiently transparent and explainable and are not well documented. Therefore, AIs used for this purpose are classified as high risk when accuracy, reliability and transparency are important to avoid adverse consequences, maintain public confidence and ensure accountability and effective redress.

In the AIA, specifically in recital 69, the need to protect the rights to privacy and to the protection of personal data during the entire life cycle of the AI is raised. Thus, the principles of minimization and data protection by design and by default are applicable when processing personal data. To ensure compliance, providers may adopt measures to anonymize and encrypt data, as well as the use of technology that allows algorithms to be brought to the data and training of AIs without requiring transmission between the parties or copying of the raw or structured data, without prejudice to the data governance requirements of the Regulation.

On the other hand, as specified in recital 71 AIA, it is essential to have understandable information on how the AIs have been developed and their performance throughout their useful life. To this end, it is necessary to make records and have technical documentation containing the necessary information to assess whether the system complies with the relevant requirements and to facilitate post-market surveillance. This information should include the general characteristics, capabilities and limitations of the system and the training, testing and validation algorithms, data and processes used, as

[338] FRA, *Facial recognition technology...* cit. pp. 23-32.

[339] The importance of data quality is highlighted in recital 67 AIA, which specifies that data of this type and its access play an important role in providing structure and ensuring the functioning of many AIs, especially when using techniques involving model training, in order to ensure that the high-risk mechanism functions as intended and safely and does not become a source of discrimination. Appropriate data management and governance practices need to be put in place to ensure that data sets for training, validation and testing are of high quality. Such data sets must be relevant, sufficiently representative, error-free and complete for the purpose of the system. Transparency is essential and attention should also be paid to reducing any biases in the datasets that may affect the health and safety of individuals, have a negative impact on fundamental rights or create discrimination. Biases may be inherent in the datasets, especially when dealing with historical data or created when systems are deployed in real settings. The results depend on such biases, which tend to increase gradually, perpetuating and amplifying existing discrimination.

well as documentation on the risk management system, clearly and completely elaborated. The technical documentation should be kept up to date during the lifetime of the instrument. In addition, high-risk AIs must allow for automatic recording of events through log files throughout the life of the system.

Linked to the above, one of the problems of intelligent mechanisms is their opacity, which makes it difficult and, in some cases, impossible to understand how they work. For this reason, transparency in the systems must be demanded from the outset. Transparency of the mechanisms appears as a transversal requirement that constitutes an essential instrument to guarantee the respect of the other protected rights[340].

Thus, they should be designed in a way that allows those responsible for deployment to understand how they work, evaluate their functionality and understand their strengths and limitations. They should be accompanied by instructions for their use, including performance characteristics, capabilities and limitations[341]. These elements would include data on the possible known or foreseeable circumstances related to the use of the high-risk AI, including the actions of the deployer capable of influencing the behaviour and operation of the system that could lead to risks to health, safety and fundamental rights, on changes that the provider has predetermined and evaluated for compliance, and on relevant human oversight measures, including those aimed at facilitating the interpretation of the AI output information by the deployers. However, transparency and instructions for use should help those using the system to make informed decisions (recital 72).

High-risk AIs need to be designed and developed in such a way that individuals can monitor their operation. It is appropriate to establish a requirement of enhanced monitoring for such systems, so that the person responsible for deployment cannot act or make decisions based on the identification made by the system, unless it has been verified and confirmed separately by two natural persons (recital 73). Thus, art. 14 AIA develops human surveillance of systems, so that they can be effectively controlled by natural persons during their period of use, which includes equipping them with appropriate human-machine interface tools. The objective of this surveillance is to prevent or minimize risks to health, safety or fundamental rights that may arise when using high-

[340] ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione...," cit., p. 159.

[341] As established in art. 13.3 letter b) AIA, such characteristics, capabilities and limitations of performance in particular have to provide for i) its purpose; ii) the level of accuracy, robustness and cybersecurity, as well as any known and foreseeable circumstances that may affect the expected level of accuracy, robustness and cybersecurity; iii) any known or foreseeable circumstances, associated with the use of the high-risk AIs according to its intended purpose or reasonably foreseeable misuse that may give rise to risks to health and safety or fundamental rights; iv) technical capabilities and characteristics of the high-risk AI to provide relevant information to explain its output information; v) performance with respect to specific individuals or groups with whom the system is intended to be used; vi) input data specifications or any other relevant information regarding training, validation and test data sets, taking into account the purpose of the system; vii) information to enable those responsible for the system to interpret the system's output information and use it appropriately.

risk AIs. The surveillance measures will have to be proportionate to the risks, level of autonomy and context of the use of the system. A very interesting issue provided for in the second paragraph of art. 14.5 AIA is that it eliminates the provision of the need for double human verification of the results issued by the mechanism when it is used for law enforcement purposes.

On the other hand, high-risk AIs must operate uniformly throughout their life cycle and have an adequate level of accuracy, robustness and cybersecurity, according to their purpose and based on the current state of the art (art. 15 AIA). Technical soundness is a key requirement. To ensure this, technical and organizational measures must be taken, for example, by designing and developing appropriate technical solutions to prevent or minimize harmful or undesirable behaviour (recital 75). Likewise, as stated in recital 76, cybersecurity is fundamental. The latter is of particular relevance, given that an AI may suffer attacks that jeopardize its integrity, and attackers may even use both the system and the data it contains for criminal purposes. For this reason, it is necessary for the instrument to be equipped with cybersecurity mechanisms that prevent it from being attacked.

Risks in systems can occur at the design stage but can also arise during their use. For this reason, recital 93 states that those responsible for deployment have an essential role to play in ensuring the protection of fundamental rights, as a complement to the obligations of the provider at the time the system is developed. Those responsible for deployment are in an appropriate position to understand the use that will be made of the mechanism, being able to detect potential risks that were not foreseen in the development, by having a more precise knowledge of the context in which it is used and the persons or groups that may be affected, including vulnerable groups of persons. Thus, art. 27 details the content that the assessment of the impact on fundamental rights must have: (a) description of the processes of the person responsible for deployment in which the system is used in line with its intended purpose; (b) description of the time period in which the system is expected to be used and the frequency; (c) categories of natural persons and groups that may be affected by its use in a given context; (d) risks of specific harm that may affect individuals; (e) description of the implementation of human supervision measures, in accordance with the instructions for use; (f) measures to be taken if the risks materialize, in particular internal governance arrangements and grievance mechanisms. The above applies prior to the first use of the system. In similar cases, the deployer may rely on prior impact assessments performed by suppliers. If, during the use of the mechanism, he or she considers that any element has changed or is not up to date, he or she must take the appropriate steps to update the information. The results of the assessment shall be notified to the market surveillance authority.

The latter must have effective investigative and remedial powers, including at least the power to obtain access to all personal data being processed and to all information necessary for the performance of its functions in high-risk AIs based on biometrics, as provided for in recital 159 AIA.

CHAPTER III

IMPACT OF FACIAL RECOGNITION SYSTEMS ON CITIZEN RIGHTS AND FREEDOMS

I. INITIAL ISSUES RELATED TO DATA SURVEILLANCE

Automatic recognition technologies have evolved so rapidly that they enable real-time remote tracking and surveillance of people and vehicles as well as the aggregation of large amounts of data on individuals and their movements, networks and relationships. This "state surveillance" is not only limited to physical public spaces but can also reach the virtual[342]. Such is the importance acquired by data in surveillance that there is even talk of "dataveillance" understood as the "systematic use of personal data to investigate or monitor the actions and communications of one or more persons"[343]. The expansion of automated mechanisms that enable the analysis of large datasets has led to the emergence of so-called "algorithmic surveillance", which refers to surveillance technologies that use computer systems to provide results beyond the raw data under analysis. It can vary in sophistication, from systems that classify and store simple information to mechanisms that attempt to predict past events, and even complex tools that compare the data collected with other data stored in databases to make matches between them[344]. The FRs fall into the latter category.

The fact that there is such a volume of data and sophisticated mechanisms capable of analysing and processing it, leads to a dangerous situation, since the subjects that have the ability to exploit AI technologies, in this particular case the RBIS in its face recognition mode, have an unimaginable surveillance power.

Some private companies such as IBM and Amazon have sold their products to LEAs to manage public order, especially in the U.S. Both have stopped marketing them because of the collision with some fundamental rights that their use entails, such as non-discrimination and racial bias, in addition to the possible mass surveillance[345]. These

---

[342] LYNCH, N. "Facial Recognition Technology in Policing and Security-Case Studies in Regulation," *Laws*, vol. 13, nº. 35, 2024, p. 1.

RENGEL exposes the term "electronic surveillance" in the field of communications, defining it as the use of electronic or mechanical devices to obtain information on the private communications and activities of individuals, mainly by LEAs and the Government. RENGEL, A. *Privacy in the 21st Century*, Martinus Nijhoff Publishers, Leiden, 2013, p. 51.

[343] MOBILI, G. "Profilazione tramite riconoscimento faciale...", cit., pp. 183-184.

[344] INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance...", cit., p. 181. Many surveillance technologies in use today have algorithmic aspects but are not fully identified with such a mechanism. This is the case with CCTV because it is limited to recording video images of the places where they are located. However, if they are equipped with a system capable of automatically comparing the faces of people captured by it with those contained in a database to detect criminals, we are dealing with an algorithmic mechanism.

[345] See, SÁNCHEZ, J. "IBM abandons facial recognition market over concerns about racial bias," *ABC*, June 9, 2020. Electronic resource obtained via the Web: https://www.abc.es/tecnologia/informatica/soluciones/abci-injusticia-y-sesgos-reconocimiento-facial-debate-abre-despues-abandono-esta-tecnologia-202006091502_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ftecnologia%2Finformatica%2Fsoluciones%2Fabci-injusticia-y-sesgos-reconocimiento-facial-debate-abre-despues-abandono-esta-tecnologia-202006091502_noticia.html, [retrieved on 10 June, 2024].

EUROPAPRESS. "Amazon extends its ban on using its facial recognition for police purposes indefinitely," May 19, 2021. Electronic resource obtained via the World Wide Web:

systems need to be studied in depth from a criminological and criminal perspective, not only in relation to the risks of violating the rights to privacy and protection of personal data, but especially because of the possibility of using the argument of guaranteeing public security to the detriment of those rights, which could lead to a situation of mass surveillance and profiling of individuals[346], as happens in some countries such as China. This situation, as we have said, severely affects basic individual rights such as privacy, personal data protection, freedom of assembly, association and free expression of thought, among others.

The fact that similar technologies are becoming more and more widespread and their use is normalized not only entails the risk of infringing the aforementioned rights, but they are also likely to cause a profound change in the social and state model, modifying the democratic state as we know it as well as its institutions[347], especially when mass surveillance is exercised secretly[348]. This would result in a "techno-surveillance society"[349] or mass surveillance in the hands of those who have the privilege of using these systems, subjecting others to unprecedented control. Thus, there is a risk of drifting into authoritarianism and restrictive decision-making in order to control the lives of others, even to the point of directing protests or anticipating them. The absence of anonymity can also discourage citizens from freely expressing their thoughts, opinions and judgments, as well as reduce their active participation in society, limiting freedom of movement and the right of assembly and demonstration. This would lead, in the most extreme cases, to the emergence of a society similar to the "Big Brother" predicted by George Orwell in his book *1984*.

Before delving into the problems that may arise from the use of FRs, especially in terms of their collision with the rights and freedoms of citizens. However, we will first address some essential issues of the face –and its image– as biometric data and its special aspects or circumstances as a parameter for remote identification by LEAs in public

https://www.europapress.es/portaltic/empresas/noticia-amazon-extiende-prohibicion-usar-reconocimiento-facial-fines-policiales-forma-indefinida-20210519121835.html, [retrieved 10 June, 2024].

[346] According to COLACURI, profiling, control and surveillance are three characteristic elements of current society. The author argues that the latest evolution of the socio-political model of capitalism has reconfigured business activity towards the acquisition of data on the behaviour of individuals to be used for commercial purposes and thus obtain greater economic benefit. The causes of this situation would be the growing digitalization that produces huge amounts of data from mobile devices. Thus, the effects of capitalism transcend the economic structure and also reach social relations. COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit. p. 124.

[347] Moreover, PRESNO LINERA, when referring to the social and democratic rule of law, also adds the consideration of digital. PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial...*, cit., pp. 51-52.

[348] CAS, J. et al. "Introduction. Surveillance, privacy and security", in Friedewald, M. et al. (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, p. 6.

[349] On the concept of "technovigilance", see CUERDA ARNAU, M.L. "La reforma de Ley de Enjuiciamiento Criminal en materia de tecnovigilancia. Overview". In Alonso Rimo, A. et al. (Dirs.). *Terrorismo, sistema penal y derechos fundamentales*, Tirant lo Blanch, Valencia, 2018, pp. 514-515. For the author, said term includes all investigative measures that involve the intervention and recording of communications, as well as investigations that use technical devices for tracking and/or geolocation, the capture in open or closed spaces of image and sound, etc.

places. This will serve as a first approach to better understand the problems derived from its use in such systems and for such purposes.

II. FACIAL IMAGES AS BIOMETRIC DATA

1. The face as a particularly sensitive private data

One of the aspects mentioned refers to the face as an element that contains sensitive information unique to the person that makes it possible to distinguish an individual from others[350] and, therefore, to identify him or her. For this reason, it is considered a particularly sensitive data. This statement has not been unanimously accepted and, sometimes, it is not considered as such, reaching biometrics in general. Thus, on the one hand, the EDPS in different Opinions recognizes that biometric data is a kind of information of an inherently sensitive nature, which is why it requires specific safeguards[351]. In addition, it emphasizes the qualification of face and fingerprints as a category of sensitive data, so that their processing should be limited to what is strictly necessary to achieve the proposed objectives[352]. Following the views of the above, Advocate General Mengozzi in *Case C-291/12* upheld the "sensitive nature by definition of biometric data"[353].

On the other hand, in the opposite direction, the A29 WP in Opinion 3/2012 on developments on biometric technologies, states that some biometric data, including the image of the face, may reveal sensitive information, such as race or ethnicity[354]. Then the WP is not recognizing that face data is a type of sensitive information but that it is susceptible to revealing it. Along the above, YUE LUI, relying on a decision by the Norwegian Data Protection Authority on the use of CCTV images on buses, explains that the images have to be processed to be capable of identifying someone. Thus, the image itself cannot be considered "identifiable", but as a carrier of personal information, not being personal information in itself. He concludes by stating that biometric data cannot be observed as sensitive data unless some measures are taken to extract genetic or health

[350] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit., p. 2.

[351] Thus, for example, Opinions of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II) (Com(2005) 236 final and COM(2005) 237 final), OJ C 91,19.4.2006, p. 43; of 18 July 2013, on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), p. 7; 3/2016 of 13 April 2016, on the Exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS), p, 8.

[352] Opinion of 07/2016 on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin Regulations), p. 9; Opinion 7/2018 of 10 August 2018, on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, p. 9.

[353] Opinion of Advocate General Mengozzi of 13 June 2013, Case C-291/12. Michael Schwarz v. Stadt Bochum. ECLI:EU:C.2013:401, p. 14.

[354] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments of biometric technologies*, 00720/12/EN WP103, 27 April 2012.

information. So it considers biometric information only as personal information that, when technically processed, becomes sensitive[355].

Similarly, but from a different perspective, JASSERAND does not consider biometric data to be sensitive *per se*, since in order to be considered sensitive they must be capable of uniquely identifying the individual and this will depend on many other circumstances unrelated to the characteristic to be measured. For example, in the case of the face, images of the face are suitable for identification if certain parameters such as light, location, exposure or camera resolution allow the image to be recognizable[356].

The legal definition of biometric data established by the GDPR in art. 9.1 and by the LED in art. 10, namely those aimed at uniquely identifying a person, leads to the exclusion of biometric templates and photographs inserted in databases until they are processed in a way that allows identification. Thus, they seem to make a distinction between personal data relating to biological or behavioural characteristics (i.e., images) on the one hand, and biometric data requiring such specific technical processing[357], on the other hand. Moreover, recital 51 GDPR explicitly excludes photographs from the definition of biometric data, as it states that "the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person". However, as SUMER states, following the technical definitions that understand all processing –even initial– of physical or behavioural characteristics that allow identifying individuals as biometric data, the images processed and inserted in databases would be logically considered as such, since their processing already constitutes the first phase of the procedure of dealing with this type of information[358].

KINDT criticizes the above distinction between personal data and biometric data because it argues that once the former has been registered, the holder loses control of its future use, not knowing what it will be. To this he adds that the nature of the data allows identification and is susceptible to biometric comparison and identification[359]. The ECHR takes a similar position in the *Case S. and Marper v. The United Kingdom* when it states that the mere inclusion of biometric information in a database has an impact on the

[355] YUE LIU, N. *Bio-Privacy. Privacy Regulations and the Challenge of Biometrics*, Routledge, Oxon, Abingdon, 2012, p. 120.

[356] JASSERAND, C. "Legal Nature of Biometric Data...", cit., pp. 307-308. The author goes on to point out, in relation to templates, that they are not capable of displaying sensitive information like the images themselves, since an image might not be regenerated from a template. So it is not certain, from a scientific point of view, that sensitive information can be derived from templates, so they may not be capable of revealing sensitive information.

[357] KINDT, E.J. "Having yes, using no? About the new legal regime for biometric data," *Computer Law & Security Review*, vol. 34, 2018, pp. 531-532.

[358] SUMER, B. "When do the images of biometric characteristics qualify as special categories of data under the GDPR: A systematic approach to biometric data processing?", *2022 Intenational Conference of the Biometrics Special Interest Group (BIOSIG)*, 2022, p. 2.

[359] KINDT, E.J. "Having yes, using no?"…, cit., p. 532.

privacy of individuals. SUMER also argues that, although facial images and other images with different characteristics are not systematically considered as biometric data, they are capable of revealing sensitive aspects of individuals and enable their identification[360], which is why they must be considered biometric data and be subject to the same rules and guarantees as the latter.

In this regard, it should be noted that at a previous time, the Data Protection Directive prior to the GDPR did not include biometric data, so they could not be understood as particularly sensitive data at the legislative level. However, authors such as KINDT already included them, especially the face, from which personal aspects such as racial or ethnic origin can be deduced[361]. Moreover, if some common data such as eating habits, which, a priori, could be considered innocuous, are sensitive data[362], even more so should the face be considered especially sensitive data because, as we have said, it allows the univocal identification of individuals.

Likewise, as they contain personal information[363], we maintain that facial images are of a sensitive nature[364] and fall within the qualification of special categories of data[365]. This follows from art. 3.13 LED, insofar as –we reiterate– it makes it possible to uniquely recognize a natural person and reveal aspects of that person (arts. 10 LED and 9.1 GDPR), extending such consideration to templates and images[366]. Moreover, recital 37 of the same body of law states that data of a particularly sensitive nature in relation to fundamental rights and freedoms deserve special protection. Such data must include those that are likely to reveal racial or ethnic origin, among which is undoubtedly the face. This statement arises from the consideration that the images of the face are a special type of personal data that contains the necessary elements to identify and individualize a subject,

[360] SUMER, B. "When do the images of biometric characteristics qualify as special categories of data under the GDPR?...," cit., p. 5.

[361] KINDT, E.J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Springer, 2013, p. 140.

[362] STITILIS, D. & LAURINAITIS, M. "Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law", *Computer Law & Security Review*, vol. 33, 2017, p. 624.

[363] In that sense, YUE LUI argues that, as biometric data are relatively unique and universal key information with which all kinds of personal information can be obtained, they would be considered sensitive information in general. YUE LIU, N. *Bio-Privacy. Privacy Regulations and the Challenge of Biometrics...*, cit. p. 121.

[364] RAJI, I.D. et al. "Saving Face: Investigating the Ethical Concerns of Facil Recognition Auditing," *Proceedings of the AAAI/ACM Conference on AI, Ethics and Society*, 2020, p. 145.

[365] Of this opinion, FRA, *Facial recognition technology...*, cit., p. 5.

[366] JASSERAND, C. "Massive Facial Database and the GDPR. The New Data Protection Rules Applicable to Research", in Leenes, R. et al. (Eds.), *Data Protection and Privacy. The Internet of Bodies*, vol. I, Hart Publishing, 2018, p. 174.

However, FRs operate with computer-generated face templates, so in LYNCH's opinion, this type of data contains less sensitive information than the image of the real face, but this does not diminish the potential impact on the right to privacy. LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit., p. 2.

In addition, recital 51 GDPR states that the processing of photographs should not be systematically considered as processing of special categories of personal data, since they are only included in the definition of biometric data when processed by specific technical means allowing the unambiguous identification or authentication of an individual.

so it does not need to be linked to a file or recording[367], i.e., it is not necessary that they have been subjected to that specific technical treatment to be considered as such biometric data.

Thus, in conclusion, the face must be understood as a type of private information that is especially sensitive because of the purpose for which it is used, that is, as information capable by itself of identifying individuals.

2. Distinction of the face with other biometric parameters: intrusiveness issues

Facial images differ from other biometric parameters in that they can be collected remotely and often without the consent or knowledge of the owner[368]. Along these lines, a distinction has been made between intrusive forms of biometric data collection and those that are understood not to be intrusive. The former include intrusions into bodily integrity such as the collection of DNA and fingerprints directly from the person, while the latter are performed remotely. It is understood that we are dealing with a less intrusive biometric technology than the others, due to the fact that automated face identification involves the recognition of other people in the same way in which this task is performed by human beings, i.e. by looking at their faces[369] and not requiring direct physical contact to capture the image[370].

However, the Court of Justice Judgment *R (Bridges) v CCSWP and SSHD* notes two similarities between facial biometrics and other parameters such as fingerprints, as it understands that both can be captured without the need for any intimate sampling and are

[367] JASSERAND, C. "Massive Facial Database and the GDPR...", cit. p. 177.

[368] SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics*, Springer, 2021, p. 22.

The intrusiveness of the techniques can be distinguished not only by the distance of data collection but also by the sensitivity of the information. In this sense, the ECHR in the *Case of P.N. v. Germany*, 11 June 2020, considers that the collection and storage of identification data in criminal cases (photographs, fingerprints and palm prints) are less intrusive to the right to respect for privacy than the storage of DNA profiles as the latter contain more sensitive information.

[369] GATES, K.A. *Our biometric future: Facial recognition technology and the culture of surveillance. Vol. 2*, New York University Press, 2011, pp. 45-46. The author states that the retinal scanner is a technique that causes particular bewilderment among users. This is because it is difficult to use, requires care to align the eye in order to capture an adequate image of the blood vessels of the eyeball.

[370] NIKLAS, P. & BARRERA, G. "Biometrics applied to public safety", *Argentine Symposium on Technology and Society (STS)-JAIIO 46*, 2017, p. 151. They further note that the face is of public information because many faces are found in official documents, the web and social networks.

Moreover, CCTV in general, excluding FRs, is considered a less invasive technique because it captures in an unobtrusive way situations that occur in the area in which it operates, and it is observed as part of the background, not as the foreground of social control. GOOLD, B. et al. "The banality of security. The curious case of surveillance cameras," *British Journal of Criminology*, vol. 53, nº. 6, 2013, p. 984. The authors conducted interviews with citizens about their views on CCTV, from which they extracted what has just been noted, as well as that surveillance cameras should not bother anyone, unless they are an individual who has a guilty conscience or is engaging in activities that they would prefer to keep hidden from the view of others.

a part of the body generally visible to the public. However, it goes on to point out that, through the use of FRs, facial biometrics can be obtained without the consent or knowledge of the individual or using force, processed on a large scale[371]. In this case, bodily integrity is guaranteed because no personal contact is required but it does entail risks in relation to informed consent and privacy. PURSHOUSE/CAMPBELL, when analysing this judgment, argue that it is wrong to consider only physical intrusion as police intrusion, since biometric and/or algorithmic technologies facilitate the use and storage of sensitive personal information by public authorities. They go on to state that FRs combine physical and informational forms of surveillance because they collect information from people's bodies, even without physical contact, and break it down into an informational structure that can be processed at a later time. For this reason, they conclude that physical contact is a poor parameter for measuring the degree of intrusiveness of a surveillance measure[372].

On the other hand, in our view, there are certain parameters such as fingerprints that are not as visible to the public as images of the face, unless there is a specific treatment that involves, as with DNA, the individual involved, who has to offer his fingerprints or collect them from a specific space such as a crime scene, making the face much more accessible to others. We also consider that its use is more intrusive and entails greater risk to rights and freedoms, not because of the actions of the subject but because the face is the part of the body most exposed to others, difficult to hide, and can be recognized from a distance[373], which places the data owner in a situation of defencelessness against those who use them for surveillance purposes. To this we must add that the collection of this information will allow its further processing.

In line with what has just been pointed out, COUCHMAN argues that real-time FRs is a technology that favours mass surveillance and that, unlike other biometric systems such as fingerprints, it can be used for passive and general surveillance that does not require the knowledge, consent or active participation of the monitored persons. If the system identifies a subject's image with the one on a list, the mechanism issues an alert. In addition, any individual can be included in a list used for facial recognition, even if he or she is not being pursued by the police or the courts. In addition, images can be collected from social networks without the data subject being aware of it[374], leading to problems with the right to privacy and the protection of personal data, as will be discussed later in the corresponding sections of this research.

[371] RAPOSO, V.L. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", *Information & Communications Technology Law*, vol. 32, nº. 1, 2023, p. 48.

[372] PURSHOUSE, J. & CAMPBELL, L. "Automated facial recognition and policing: A *Bridge* too far?", *Legal Studies*, vol. 42, 2022, pp. 222-223.

[373] DUSHI, D. "The use of facial recognition technology in EU law enforcement: Fundamental rights implications", *Global Campus of Human Rights. South East Europe*, Policy Briefs, 2020, p. 8.

[374] COUCHMAN, H. "Mass Surveillance on Our Streets: Facial Recognition and the Threat to Our Rights," *European Human Rights Law Review*, nº. 6, 2019, p. 585.

Similarly, LYNCH acknowledges that live facial recognition is a very intrusive technique as cameras scan individuals on the street and compare their images with those collected from a list of persons of interest[375]. He goes on to assert that the impact on society and individuals depends on use cases and context as well as informed consent, implications on the decision or outcome, and issues relating to storage and subsequent use[376].

For some authors, the fact that face recognition is performed remotely without the need for any type of physical contact, rather than posing a threat, is an advantage[377]. However, in our opinion, in addition to the problems related to intrusiveness, it has some serious limitations as it does not have the same level of accuracy compared to DNA, to which must be added the lack of knowledge of the frequency with which facial elements appear in the population. Moreover, the technique is limited by issues related to the conditions under which the image is taken and the quality of the image, the cameras used and the size of the database. In addition, it must be taken into account that the face may change over time, which could lead to errors in identifications, especially when the systems are used in uncontrolled environments[378].

Returning again to the issue that concerns us at this point and, in view of everything mentioned so far, we understand that the collection and processing of all types of biometric data entails an invasion in the private sphere of the individual, whether taken remotely or personally. Thus, following the concept of biometric identification established in recital 15 of the AIA, there is practically no distinction between intrusive and non-intrusive biometric identification, while recognizing that all biometric data constitute a type of sensitive information[379]. This is because the said recital defines it as "the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not". Therefore, encompassing all biometric parameters without distinction within the term biometric identification, we understand that the AIA treatment of all of them is equal, which is why they all share identical characteristics. Likewise,

[375] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit. pp. 3-4.

[376] *Ibd.*, p. 4.

[377] SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics...*, cit., p. 22. GATES notes another advantage of FRs in comparison with other biometric data, linked to remote identification. In this case, it would be the connection with forms of documentary identification, as he understands that inserting the technology into identification systems would allow taking advantage of existing bureaucratic rules and practices because billions of photographs of faces are circulating in documents and police files. Integrating this data into video surveillance cameras would facilitate remote identification and automate the task of monitoring such systems, helping to increase their scale and reach. GATES, K.A. *Our biometric future...*, cit., pp. 46-47.

[378] *Idem.*

[379] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit., p. 3.

their collection, storage and processing is intrusive, regardless of the type of information involved.

In another line, the databases used should be highlighted. Unlike DNA, agents do not need to obtain suitable templates for face recognition from databases specifically created for that purpose. What this means is that there are already repositories held by LEAs (such as driver's license and passport photographs) that are integrated into the FR technology. In addition, police images of suspects or criminals are available, as well as the huge amount of photographs that individuals themselves have shared on social networks (making their face public)[380], which are susceptible to being captured and collected in databases with the aim of being used to identify individuals in the police field. Thus, FRs is a tool with a high identification potential that has been rapidly adopted and integrated with existing data systems. The use of images from police databases does not entail major privacy issues, while the use of images from social networks or images captured by CCTV in public places is a different matter.

3. Availability of the face in public places

The face is constituted as the fundamental element of identification among individuals. Nowadays, in the information and surveillance society, the face, as a sign of identification par excellence, can be linked to other types of personal information such as a name and it is even possible to know the political ideas or understand the state of mind of a person[381]. Transforming expressions into data implies going beyond traditional identification, getting to the core of personal identity, understood as a set of convictions, thoughts and feelings that qualify each individual[382]. Thus, with biometrics, recognition, which was initially an intuitive process derived from human interaction, has become automated, the body or its various component parts becoming mere data. Thus, it becomes a simple object that is controlled by another[383] and whose identity is determined through the language of mathematics.

---

[380] SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics*..., cit., pp. 23-24. The authors highlight the case of Australia. In this country, the use of FRs has been made possible since 2017. Its legislation allows federal agencies to search and share images of driver's licenses, passports, etc. On the other hand, since 2015 FRs can be used for the investigation of major crimes or terrorist attacks without a search and arrest warrant even without the knowledge of the interested parties.

There are authors who consider that databases that take images from social networks that the individual has published do not deserve the same level of protection as other sensitive data. However, from the moment that the subject has not given his consent and even unaware that they are being used for other purposes of which he is not aware, we understand that they should be treated identically to the others. JASSERAND, C. "Massive Facial Database and the GDPR...", cit. p. 183.

[381] RAFFIOTTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità...", cit. pp. 383-384.

[382] *Ibd.*, pp. 384.

[383] As a result, there is a risk of individuals losing control over their own data. Of this opinion, WOODWARD, J.D. *Super Bowl surveillance...*, cit., p. 5.

Being a digital representation of the human being, like all other data inserted in a computer, it can be easily reproduced, transmitted, analysed and reused, while the holders of such data have little or no control –sometimes not even knowledge– over whether and how the processing affects them in their real life. Biometric data are not like other personal codes such as those inserted in documents like passports, since the latter, although capable of identifying a subject, do not derive from a bodily part of the subject[384], i.e., they do not turn the body into a mere alphanumeric code, so they do not entail the process of reification or dehumanization that biometrics do[385]. This is because, as mentioned above, the owner of the data ceases to have control over it, leaving its use in the hands of others. Therefore, both types of data are different, the processing of the latter constituting a superior invasion into the sphere of the private life of individuals.

As noted in the previous section, not all biometric data are equally visible or accessible. The face is one of the most exposed –if not the most expose– to identification. It follows that, when a person is in a public space, he or she is making his or her face available for others to see. Not only to individuals, but also to surveillance systems. CCTV is widely used today, whether in the public or private sphere. Identification performed by individuals interacting with each other would not be as intrusive as the monitoring and control activity performed at the state level using[386] technology such as FR, since the short and long term impact is much higher in the latter case, due to the massive information processing capacity in a very short time and the potential severity of the results.

The processing of biometric data is prohibited under both the GDPR and the LED with certain exceptions. One of them is when the holder makes them manifestly public (art. 9.2 e) GDPR and 10 c) LED). In this case, the question arises as to what happens when the individual is in a public place such as a street equipped with video surveillance systems that have built-in FR mechanisms. In such a case, nothing would prevent such mechanisms from recognizing the image of his face since it is a data that the owner is clearly making public and susceptible to capture.

The Judgement of ECHR *Case of P.G. and J.H. v. The United Kingdom*, when it held that a person walking down the street will inevitably be visible to any member of the public who is also present. Surveillance by technological means of the same public scene

[384] However, in YUE LIU's view, the difference between the two types of data is because the codes and numbers linked to certain documents are unique and relatively stable. YUE LIU, N. *Bio-Privacy. Privacy Regulations and the Challenge of Biometrics...*, cit. p. 69.

[385] BREY, P. "Ethical aspects of facial recognition systems in public places...", cit., p. 107. The author states that the functional reduction of body parts into information makes them acquire a new meaning or function since they allow the identification of individuals when they are inserted into intelligent systems and are comparable to other identifiers. Added to this is the use and control by others of this information. In this sense, the face no longer belongs to its owner but to those who process it. He adds that, even if individuals possess it, if they do not understand how the technology works, they cannot use it. So that part of the body is not completely theirs because it has acquired a new meaning that is incomprehensible to the individual holder.

[386] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit., p. 3.

is of a similar character. Privacy issues may arise here, whereby files collected by LEAs would have to be protected under art. 8 of the Charter.

However, following the previous judicial pronouncement, we understand that, as with DNA or fingerprints, FR technology allows the extraction of unique information about an individual, which makes it possible to accurately identify him or her in different circumstances. Taken in isolation or in conjunction with other metadata, FRs are an important source of personal information that is inherently private. He goes on to state that, the fact that the data is derived from characteristics of the individual's face that are "manifestly public", does not detract from the above. Therefore, while recognizing that the face is a type of information that becomes manifestly public in view of others when in a common space, it is no less true that there is a private sphere or realm in the sense that it must be left to the subject to decide whether he wants to expose his face to surveillance systems[387]. For this reason, information and consent are of particular importance. In a similar sense to the previous pronouncement, RAPOSO argues that, just as there is a reasonable expectation of privacy in one's own home (a private space par excellence) and this is violated when the government installs cameras in a personal home, the same happens when a person is in a public space. In this case, the mere fact of being in the outside world should not open the door to submit to this type of surveillance[388]. All these issues will be dealt with in greater depth below, but it was necessary to introduce them at this point, as a basis for what will be discussed later.

III. IMPACT ON FUNDAMENTAL RIGHTS AND FREEDOMS

Respect for fundamental rights is at the core of trustworthy AI[389], as stipulated by the High-Level Expert Group on AI in its *Ethics Guidelines for Trustworthy Artificial Intelligence*. However, they can often be restricted or even injured by the use of AIs. This is one of the problems that intelligent mechanisms entail and is especially significant in FRs as their police use not only impacts fundamental rights and freedoms at the individual

[387] The *R (Bridges) v CCSWP and SSHD* judgement was motivated by this very fact, given that the South Wales Police had implemented FRs at two different times when the claimant could have been identified by such mechanisms, as at no time did he consent to this taking place and further alleges that he was not properly informed.

[388] RAPOSO, V.L. "Health, privacy and liberty: a call for digital governance during (and after) the pandemic", *The International Journal of Human Rights*, vol. 27, no. 3, 2023, p. 533.

[389] At this point, it is necessary to clarify what the terms human rights and fundamental rights refer to, since they are sometimes used interchangeably. On the one hand, the former encompasses the rights inherent in the nature of a person, who possesses them by the mere fact of being a person and are directly connected to dignity. Thus, a right is a power that the holder of the right has to do something or prevent a certain activity; and, on the other hand, fundamental rights are identified with the previous ones but, in this case, they are contained in a specific legal system, normally in the Constitution of the State in question. Thus, the latter are the cornerstone on which a public system is based. A system will only be considered democratic if it adequately provides for and guarantees these rights. FERNÁNDEZ RODRÍGUEZ, J.J. "El encuentro entre seguridad y derechos humanos: Actualidad y problemas", *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 14, nº. 1, 2019, p. 90.

but also at the societal level, affecting collective rights as well, so they are capable of reaching our social and democratic political stability[390]. The AIA lists those that are most harmed by their use, all of which must be taken into account when classifying instruments according to risk. Among those most endangered by FRs when used in the public sphere for law enforcement purposes are human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and association, and non-discrimination[391]. The need to prevent *ex ante* the infringement of these essential fundamental rights cannot be seen in a solely individual dimension, as the interdependence between them, their social value and their inseparability from the protection of the rule of law and democratic principles must also be considered[392].

The use of FRs is susceptible to violate fundamental rights even if the requirements and limits established in the AIA are followed. It is true that those are not absolute and can be limited as long as a series of requirements such as proportionality and necessity of the measure are observed. Furthermore, any limitation should only be accepted when other fundamental rights or public interests are considered to be prevalent. In our specific case, the argument of maintaining security could act as a spring to legitimize the use of FRs in public places. Therefore, in the remainder of this research, we will address the rights and freedoms of citizens that may be compromised by the use of FRs and the issues related to security and surveillance. The former in this third chapter, while the latter will be dealt with in the following chapter.

With regard to rights and freedoms, these have been divided into different blocks. Firstly, the individual rights of persons in their private aspect: dignity, privacy, protection of personal data, personal identity, self-image and freedom of movement; individual freedoms in the social sphere: expression and, as a manifestation of this, assembly, demonstration and strike. Because of its importance, a separate section has been devoted to the analysis of the right to non-discrimination. In addition, the right to the presumption of innocence will be addressed and, finally, we will refer to some of the new rights that are appearing as a result of the new digital society. After this, the following section will deal with the circumstances that may legitimize their limitation and, finally, some additional problems arising from FRs will be discussed.

---

[390] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 2.0*, adopted on 26 April 2023, p. 5.

[391] Recital 48 of the AIA lists all the rights that may be harmed by AI mechanisms, among which are, in addition to those mentioned above, the right to effective judicial protection, the right to intellectual property, etc.

[392] SCHEPISI, C. "Diritti fondamentali, principi democratici e *rule of law*...", cit., p. 207.

The owners of the data have the expectation that the processing of the same will be legitimate and in accordance with the regulations. In this case, it follows the provisions of the legislation on personal data protection, which establishes the limits and requirements that must exist for its processing and treatment to be adequate. See, more extensively, PORCEDDA, M.G. "On boundaries-Finding the essence of the right to the protection of personal data", in Leenes, R. et al. (Eds.), *Data Protection and Privacy. The Internet of Bodies*, vol. I, Hart Publishing, 2018, pp. 277-312.

1. Human rights in their private dimension

1.1.Human dignity

The importance of the protection of human dignity is unquestionable since the Preamble of the Universal Declaration of Human Rights adopted and proclaimed by the United Nations General Assembly in its Resolution 217 A (III), of 10 December 1948, declares that "whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world". It goes on to state that the peoples have reaffirmed in the Charter their faith in fundamental rights, in the dignity and worth of the person. Furthermore, in its first article, it states that "all human beings are born free and equal in dignity and rights".

At the European regional level, it also appears as one of the indivisible and universal values on which the European Union is founded, whose action always has the person at the centre. In this sense, Title I of the Charter is devoted to this right and, specifically, Article 1 on "human dignity" establishes that it is inviolable and must therefore be respected and protected. For this reason, it is the essential pillar on which all other rights and freedoms are based.

However, the Convention does not expressly include dignity among the rights and freedoms protected therein, but the ECHR has stated that respect for human dignity and freedoms constitutes the "very essence" of its objectives[393]. This is because the lack of effectiveness of the rights guaranteed in the Convention is likely to result in the dehumanization of the individual[394].

The AIA also places the protection of dignity in first place as the main right[395] from which all other rights emanate. In different recitals of the AIA, reference is made to this right and the need to protect and respect it. Thus, in number 27, when it refers to the need for human action and supervision, it establishes that AIs are a tool that must respect it; in number 28, it mentions the possibility that the instruments may be used in an incorrect and harmful way against the values of the EU, among which is human dignity. Number 31 is devoted to scoring systems, which can undermine this right and the right to non-discrimination as well as the values of equality and justice. In classifying systems as high-risk, account is taken of the magnitude of their impact on the fundamental rights protected by the Charter, with dignity being mentioned first in recital 48.

But what is human dignity? This concept is one of the basic pillars of law, transcendental, and serves as the foundation of what is to be considered a human right in

[393] Judgement of the ECHR, *Case C.R. v. The United Kingdom*, 22 November 1995, no. 20190/92.

[394] FULCHIRON, H. et al. "Vie privée et familiale", *Journal Europeen des Droits de l'Homme*, nº. 1, 2021, p. 246.

[395] FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?...*, cit., p. 47.

general[396]. This is so because dignity is the basis of all other rights and a rule that violates it cannot be considered valid[397]. Despite being essential, this is a term that is difficult to define because it is diffuse and this makes it difficult to determine, characterize and define[398]. Moreover, it is the result of the confluence between philosophy and law. Thus, in the field of philosophy of law, dignity has its roots in modernity, which imposes humanism and places the individual at the centre[399]. Thus, the dignity of the person is the human quality itself and prevents individuals from being treated as mere objects[400]. By virtue of it, what is human is distinguished from what is not, so that, in the opinion of MARÍN CASTÁN, dignity appears as a sign of identity of individuals as beings endowed with intelligence and freedom, as moral beings[401].

In this sense, dignity, as a proper and exclusive quality of every person, translates into the ability to decide his or her conduct freely and rationally, with the consequent respect by others[402]. Dignity is inviolable because it cannot be taken away but it can be injured by others when it is not respected[403]. From the ethical point of view, it has a general validity and, in a democratic society, its survival keeps human rights alive[404], since the exercise of these rights will depend on respect for dignity. Thus, it is the structural element that should guide legal and normative solutions[405].

The RBIS and, more specifically, the FR impacts on the dignity of the individual as it interferes with subjective fundamental rights and also collectively, affecting the

[396] SPAEMANN, R. "Sobre el concepto de dignidad humana", *Persona y Derecho*, nº. 19, 1988, p. 16.

[397] ATIENZA, M. *Sobre la dignidad humana*, Editorial Trotta, Madrid, 2022, p. 1.

[398] MARÍN CASTÁN, M.L. "La dignidad humana, los Derechos Humanos y los Derechos Constitucionales", *Revista de Bioética y Derecho*, nº. 9, 2007, p. 1.

[399] PAVIA, M.L. "La dignité de la personne humaine", in Cabrillac, R. et al. (Dirs.), *Libertés et droits fondamentaux*, Dalloz, Paris, 2007, p. 145.

[400] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 15.

[401] MARÍN CASTÁN, M.L. "La dignidad humana...", cit., p. 1. Years before, SPAEMANN expressed himself in a similar way, when he considered dignity as a personal quality, as a way of behaving. SPAEMANN, R. "On the concept of human dignity...", cit., p. 16. He exemplifies the fact that the dignity concerned lacks the naturalness essential to all dignity with the profession of actor, considered unworthy for some time because the actor, in the exercise of it, stages his characters, so it is not an immediate expression of his own being.

[402] MARÍN CASTÁN, M.L. "La dignidad humana...", cit., p. 2.

[403] SPAEMANN, R. "On the concept of human dignity...", cit., p. 17. On p. 18, the author maintains that dignity cannot be taken away, but that the only thing that can be taken away is its external manifestation.

[404] PAVIA, M.L. "La dignité de la personne humaine...", cit., p. 164. The author, after analysing throughout the chapter the evolution of dignity at the international level and in France, concludes that its survival and constant evolution has led to its lack of definition but, at the same time, has kept it present.

[405] COTINO HUESO, L. "Nuevo paradigma de las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", in Cotino Hueso, L. (Dir.), *Derecho y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, p. 71. The author goes on to state that, in a positive sense, AI and disruptive technologies should be oriented towards the effective achievement of dignity and rights. Moreover, from the former, the legal and ethical values and principles of AI can be derived. While, from a negative point of view, it is necessary to offer guarantees against the risks and impacts of these techniques on dignity and rights. Thus, the former acts as a legal limit and, from it, new fundamental rights or new contents and guarantees of existing ones can be derived.

political order and social peace[406]. More specifically, the collection, measurement and processing of biometric data can damage the personal feeling or experience of dignity, as individuals may feel uncomfortable with surveillance through biometrics[407] and, therefore, see this right affected.

Along these lines, an essential issue to be taken into account for the purposes of our study is that public order can only be conceived in conjunction with the concept of dignity. Where the former is expressly invoked, the dignity of the person is not far behind[408]. In this context, dignity has two versions, one individualistic and the other specific. In the first, dignity is the eminent value attributed to each individual, taking into account the unique and irreplaceable character of his or her personal realization. Therefore, it consubstantially links dignity to freedom. Since it is understood that through the latter, the personal fulfilment of each subject is sought, the concept of dignity –as we have already pointed out above– is the basis for all other fundamental rights. It is thus conceived as a shield that seeks to protect them[409]. For its part, the second consists in defining dignity as the eminent value attributed to the human being as a member of the human species. From this perspective, the objective of preserving dignity is predominant over that of favouring the individual[410]. We consider dignity in its first meaning, i.e., individual, because it is more closely linked to the approach established in the AIA linked to dignity as the source from which the other rights and freedoms of citizenship emanate.

Another fundamental aspect in relation to dignity is the risk of reductionism of the individual to a simple code to make him machine-readable[411] when his biometric data is extracted and the fact of knowing whether the new identification methods respect identity as an essential element of dignity[412]. As we pointed out above in relation to the face and its conversion into a mere piece of data when used in FRs, problems arise linked to the possible dehumanization or objectification of the individual –more specifically of his face[413]– and the use of this information by others, who cease to be the owner of it.

---

[406] COTINO HUESO, L. "Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection...", cit., p. 359.

[407] SPROKKEREEF, A. & HERT, P. "Biometrics, Privacy and Agency...", cit. p. 92.

[408] LEBRETON, G. "Ordre public et dignité de la personne humaine: un problème de frontière", in Redor, M.J. (Dir.), *L'ordre public: Ordre publico u ordres publics? Ordre public et droits fondamentaux*, Bruylant, Bruxelles, 2001, p. 353. The author, in the following pages of the chapter, links dignity with public morality whose main function is to contribute to the maintenance of social peace and not to moralize the subject.

[409] *Ibd.*, p. 355. Similarly, GARCÍA TOMA, V. "La dignidad humana y los derechos fundamentales", *Derecho & Sociedad*, nº. 51, 2018, p. 14. The author affirms that dignity is inherent to each and every human being and does not admit substitution or equivalence. Therefore, it is the sustenance of constitutional rights and those established in international treaties.

[410] LEBRETON, G. "Ordre public et dignité de la personne humaine...", cit., pp. 355-356.

[411] COTINO HUESO, L. "Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection...", cit., p. 359.

[412] BYK, C. "Biométrie et Constitution: est-il déjà trop tard pour les libertés publiques?", *La Semaine Juridique-Édition Generale*, no. 25, 2008, p. 20.

[413] *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 15.

The EDPS in *Opinion 4/2015 toward a new digital ethic. Data, dignity and technology*, puts dignity at the heart of the new digital ethic. It considers that greater respect for this right and more safeguards can act as a counterbalance to pervasive surveillance and power asymmetry. It therefore reaffirms that it must be at the heart of the new digital ethic[414]. It is therefore essential that all RBIS and, more specifically, FRs respect the dignity of individuals when they are intended to be used especially in public spaces for law enforcement purposes, with LEAs having to make an impact assessment between the potential harm to it and the consequent benefits in terms of maintaining security.

1.2.Privacy

Privacy is one of the rights most compromised by the use of FRs in the public sphere for law enforcement purposes, since facial characteristics are not secret and can be collected covertly, preventing the anonymity of individuals in a particular situation[415]. Its endangerment already has serious consequences not only at the individual, but also at the social level, since it is a precondition for the development of democracy and freedom[416], as well as for the exercise of other fundamental rights and freedoms of citizenship[417], such as personal identity and self-image, movement, demonstration, etc.

1.2.1. Approach to the concept of privacy

Private life can be understood in two senses. On the one hand, as the hidden life, at least discreet, which is opposed to public life insofar as the latter takes place in the street or in a place accessible to others; but, despite what has been immediately pointed out, this does not mean that private life is only that which takes place in the home, but rather refers to life in serenity[418]. And, on the other hand, it is identified with the ability

[414] EDPS, *Opinion 4/2015 Toward a new digital ethic. Data, dignity and technology*, 2015, pp. 14-16.

[415] PRABHAKAR, S. et al. "Biometric recognition...", cit. p. 41.

[416] NAKAR, S. & GREENBAUM, D. "Now you see me. Now you still do: Facial recognition technology and the growing lack of privacy," *Boston University Journal of Science and Technology Law*, vol. 23, nº. 1, 2017, p. 101.

[417] CAS, J. et al. "Introduction. Surveillance, privacy and security...", cit., p. 1. The authors point out that it is a precondition for expressing oneself and thinking freely, especially now, with the rise of the media and social networks. They further argue that whether the Internet can continue to be an infrastructure for communication and unrestricted access to information, whether it supports freedom of expression and political participation or whether it becomes an instrument of surveillance and control, depends on respect for privacy.

[418] BEIGNER, B. "La protection de la vie privée", in Cabrillac, R. et al. (Dirs.), *Libertés et droits fondamentaux*, Dalloz, Paris, 2007, pp. 189-190.

of individuals to decide that what makes up their private life is not known by others[419] making public only what is considered appropriate[420]. We are therefore dealing with a right related to individual freedom as a claim against society.

It is considered the heart of human rights as an essential component of the others[421]. Thus, we find ourselves before a universal personal right linked to the dignity of the person[422] and to the protection of personal autonomy[423] and identity[424]. In this sense, it appears as an autonomous but instrumental right to guarantee the previous rights in a broad sense[425]. The link with the former is clear, insofar as autonomy delimits the private informational and observational space, while privacy consists of the right to control the private sphere and to decide who to exclude and who not to exclude from it. Therefore, the right to privacy consists in keeping organizations and other individuals (autonomy) away from access to personal information and images, as well as from their

[419] *Ibd.*, p. 191. RACHELS, J. "Why privacy is important", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, p. 14. According to the latter author, the value of privacy is based on the idea that there is an intimate connection between our ability to control who has access to us and our information, and the ability to create and maintain different types of social relationships with different people.

[420] BARKER, R.B. "A definition of privacy", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, p. 281. The definition defended by the author is that of privacy as control over when and by whom others can feel the various parts of us. He understands the verb to feel as seeing, hearing, touching, smelling, etc.

Along with the sphere of life that remains hidden from others, it carries the intrinsic benefit of preserving one's sense of self. RENGEL, A. *Privacy in the 21st Century*..., cit., p. 32.

The term privacy by itself may be an abstract concept, which makes it difficult to define, but what is certain is that all humans need to know that certain aspects of their private life will be –redundancy aside– private and hidden from others. With the advance of ICT it is difficult to know the extent of this fundamental right or even if it exists. HUMBLE, K.P. "International law, surveillance and the protection of privacy", *International Journal of Human Rights*, vol. 25, nº. 1, 2021, p. 4.

[421] HIRANANDANI, V. "Privacy and security in the digital age: Contemporary challenges and future directions", *The International Journal of Human Rights*, vol. 15, nº. 7, 2011, p. 1091.

[422] PAREJO ALFONSO, L. "El derecho fundamental a la intimidad y sus restricciones", in López Ortega, J.J. (Dir.), *Perfiles del derecho constitucional a la vida privada y familiar*, Consejo General del Poder Judicial, Madrid, 1996, p. 30; HEVAL ÇINAR, O. "The current case law of the European Court of Human Rights on privacy: challenges in the digital age", *The International Journal of Human Rights*, vol. 25, nº. 1, 2021, p. 26.

[423] NORTH-SAMARDZIC, A. "Biometric technology and ethics: Beyond security applications", *Journal of Business Ethics*, vol. 167, nº. 3, 2020, p. 439. This autonomy is also linked to individual liberty, in that all people must be free to make vital decisions for themselves, which implies freedom from sovereign intrusions. In the realm of AI, it requires mitigating illegitimate coercion whether direct or indirect, threats to mental autonomy and health, unwarranted surveillance, deception, and unfair manipulation. *Ethics Guidelines for Trustworthy Artificial Intelligence*, para. 42.

[424] HUMAN RIGHTS COUNCIL, *The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights.* Forty-eighth session, 2021, p. 3.

Similarly, GUO, Z. & KENNEDY, L. "Policing base don automatic facial recognition", *Artificial Intelligence and Law*, vol. 31, 2023, p. 397, when they argue that individual harms to dignity, privacy and autonomy combine and constitute a form of cultural harm that directly impacts individuals and society as a whole; & ARENAS RAMIRO, M. & DÍAZ LIMA, D. "Privacidad y derechos digitales", in Balaguer Callejón F. & Cotino Hueso, L. (Coords.), *Derecho público de la Inteligencia Artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios del Estado Autonómico, Zaragoza, 2023, p. 290.

[425] DE LA MATA BARRANCO, N.J. & BARIÑAS UBIÑA, D. "La protección penal de la vida privada en nuestro tiempo social: Necesidad de redefinir el objeto de tutela?", *Revista de Derecho Penal y Criminología*, nº. 11, 2014, p. 41.

observation and monitoring[426]. As for identity, it should be remembered that since the face is the element of identification par excellence, it constitutes one of the parameters of personal identity, so that individuals have the right to control the images of themselves[427], i.e., to decide who is shown and authorized to be treated and who is not.

It is included in international texts on the protection of human rights. Among others, in art. 12 of the Universal Declaration of Human Rights, art. 17 of the International Covenant on Civil and Political Rights; and, at the European level, in art. 8 of the Convention and 7 of the Charter[428].

Combining the two aforementioned perspectives on the concept of privacy, it can be described as the right to be left alone but also as the ability to protect oneself from unwanted access by others (including the State itself, which also has to guarantee privacy[429]), exercising control over personal information[430] and intimate relationships, as well as the protection of one's personality[431]. We are therefore dealing with a right that has a negative and a positive aspect. The first, as a "right to be left alone" and, the second, in the sense of allowing the individual to develop his personality and the affirmation of his individual freedom[432].

The judgment of ECHR *Case Von Hannover v. Germany (nº. 2),* compiling the existing case law up to the date it was issued, establishes that the notion of private life contains elements relating to the identity of a person, among which are his photograph, his physical and moral integrity. The guarantee offered by art. 8 of the Convention is primarily aimed at ensuring the development without external interference of the personality of every subject in relation to others. Thus, it concludes, there is a zone of interaction between the individual and others which, even in a public context, may form

[426] SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics*, Springer, 2021, pp. 29-30.

[427] *Ibd.*, p. 30. The authors point out that individuals can exercise control in their interpersonal contexts and, therefore, over to whom they show their face.

[428] For this reason, NORTH-SAMARDZIC, A. "Biometric technology and ethics...", cit., p. 439, understands privacy as a legal rather than an ethical issue, since there is a regulatory framework that protects it.

[429] HUMBLE, K.P. "International law, surveillance and the protection of privacy...", cit., p. 5.

[430] In this sense, HIRANANDANI refers to "information self-determination" as the ability to control the flow of personal information. He also places this right as the basis of democracy because it represents the dividing line between the State and individuals. HIRANANDANI, V. "Privacy and security in the digital age...", cit. p. 1092.

[431] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit., p. 5; PAREJO ALFONSO, L. "El derecho fundamental a la intimidad y sus restricciones...", cit., p. 17. Thus, privacy has both a negative aspect when sharing certain information with others is rejected, and a positive one when it is shared.

[432] DE LA MATA BARRANCO, N.J. & BARIÑAS UBIÑA, D. "La protección penal de la vida privada en nuestro tiempo social...", cit., p. 31.

part of his private life[433]. The latter is particularly affected when the recording of images is carried out clandestinely for police investigation purposes[434].

1.2.2. How privacy is affected by FRs

Technological developments in the 21st century have led to increased surveillance in the private sphere of individuals[435]. Even in democratic regimes, surreptitious surveillance has been developed under the justification of the need to protect national security and prevent crime and public disorder[436], using novel techniques, including FRs, which may collide with rights. In the current digital society, the traditional idea of privacy has been modified[437], seeing ourselves limited to algorithms that contain our personal (and non-personal) data. This information increases daily with the use of electronic devices, travels, is shared and can sometimes be linked to other types of data that will be used and controlled by others, resulting in an unprecedented domination of society.

The main privacy issues that arise in relation to the use of facial information when using facial recognition mechanisms are linked to the way in which biometric information is obtained, retained, stored and shared. The technology that relies on this data interferes with the right analysed here by identifying individuals and allowing information about them to be linked and connected between databases[438] (which will be studied in greater

[433] ECHR Judgment *Case Von Hannover v. Germany (no. 2)*, February 7 2012, nº. 40660/08 & 60641/08.

In this line, NISSENBAUM argues that the fact that it is understood that privacy could be violated in the public sphere is largely due to the way in which the terms "public" and "private" have been used in political and legal theory; while the latter refers to the family and other intimate personal relationships, the former refers to the civic or community environment. NISSENBAUM, H. "protecting privacy in an information age: the problem of privacy in public", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, pp. 185-186.

For his part, MARSHALL considers that a distinction is made between private and public life. MARSHALL, J. *Personal Freedom through Human Rights Law*, Martinus Nijhoff Publishers, Leiden, 2009, p. 50. But we do not understand this to mean that there is a difference between public and private space, but rather that the sphere of the individual's private life is different from that which he manifestly makes public, whether in an intimate or public sphere.

[434] LÓPEZ ORTEGA, J.J. "La protección de la intimidad en la investigación penal: necesidad y proporcionalidad de la injerencia como presupuestos de validez", in López Ortega, J.J. (Dir.), *Perfiles del derecho constitucional a la vida privada y familiar*, Consejo General del Poder Judicial, Madrid, 1996, p. 303.

[435] HEVAL ÇINAR, O. "The current case law of the European Court of Human Rights on privacy...", cit., p. 26. Similarly but years earlier, ARCHARD, D. "The value of privacy", in Claes, E. et al. *Privacy and the Criminal Law*, Intersentia, Antwerpen, 2006, p. 14. The latter believed that the increased threat to privacy was due to the evolution of more efficient methods of collecting, processing and storing information.

[436] ALDERSON, J. *Human Rights and the Police*, Council of Europe, Strasbourg, 1984, p. 62.

[437] The right to privacy, in our time, is one of the most important fundamental rights. KUGELMANN, D. & KOSIN, C. "Surveillance powers of the police and the protection of personal data", Alleweldt & Fickenscher (Eds.), *The police and international human rights law*, Springer, 2018, p. 156.

[438] MANN, M. & SMITH, M. "Automated Facial Recognition technology...", cit., pp. 130-131.

depth below in the analysis of the right to the protection of personal data). In addition, the face is a parameter that is very difficult to hide and alter and is linked to one's physical existence. Thus, FRs interfere with the right to privacy from the moment in which other people and organizations possess personal information about the face and by observation/perception through such devices.

The above is of great relevance in relation to the systems that are the subject of our study, namely those used by LEAs in public accessible places, since their inclusion in CCTV as a surveillance mechanism can lead to a massive and indiscriminate collection and processing of personal information, posing a great threat to rights. This is how the ECHR understands it in the judgment *Case of Glukhin v. Russia* (first pronouncement in which an international Court pronounces on facial recognition technology) when it states that "biometric mass surveillance, in particular with the use of facial recognition technology, represents one of the greatest threats to fundamental rights in the digital age". In addition to the above, individuals may not have consented to such processing of personal data[439]. Therefore, it may be in their minds that such information remains hidden from others, including intelligent systems, which is why their right to privacy is being violated.

Because of the controversies that arise in relation to the capture of images in the public sphere, the following will address the issue of privacy in the public sphere and the use of surveillance systems.

1.2.3. Privacy in public space and the interference with the use of FRs

It is in the social sphere of coexistence that the public and private spheres converge, blurring the boundaries that define each of them. Human beings interact in a common space where the right to privacy has virtuality, where it acquires full meaning because, in order to be effective, individuals have to decide which aspects of their lives they keep away and hidden from others, those that they make manifestly public. The problem arises when the performance or certain aspects of life are developed in the public space in full view of others.

In such a line, what happens, is all expectation of privacy lost and all matters surrounding the individual become public knowledge, is the recording and processing of personal data by surveillance systems consented to merely because it occurs on the street?

The Constitutional Court of France Judgement nº. 2012-652 DC, 22 March 2022 considered that the maintenance of a database with biometric identity information that allows identification interferes with the right to privacy.

[439] This situation, in COLACURI's opinion, can lead to mass surveillance in the absence of any form of consensus of the individuals under treatment. COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit. p. 127.

Despite the fact that, traditionally, individuals have a lower expectation of privacy in public places compared to private sphere or spaces away from the view of third parties, there are situations where there is a reasonable expectation of privacy in those[440] without people being subject to surveillance. Therefore, this right cannot be evoked only in the home or away from others because, following LÓPEZ ORTEGA, this would mean "an unjustified restriction in the scope of protection (...) that not only attends, as a delimitation criterion, to the spatial scope in which the private life of the person develops, but also to the insidiousness of the means used to discover the intimate acts or facts"[441].

New surveillance mechanisms make social contexts ambiguous because people have to protect their privacy in public space in a way that may reduce the potential for social interaction and the real value of these environments. This situation impacts democracy, making it insecure[442].

What we have just pointed out has not been a unanimously accepted position and, ACHARD in the case of CCTV (in general, without mentioning the FRs inserted in them, which would significantly increase the issues to be pointed out) in public spaces, considers that it does not interfere in the field of privacy or provide others with the opportunity to directly perceive acts that should not be seen. These instruments provide surveillance in the places indicated and are usually publicly identifiable. He goes on to point out that any act that a subject performs in a video-surveilled place and is detected by such devices is executed consciously and voluntarily[443]. On the other hand, MARSHALL –with a more accurate criterion– is critical of the above, in the sense that he understands that it is not clear whether being captured by CCTV is something that is done voluntarily only if the cameras are "publicly identifiable", because the fact of knowing that they are in a certain place does not mean that the recording of the personal image is consented to, implying an invasion of privacy in the case of not having given consent to it[444]. Moreover, the fact of not being able to see who is watching us may disturb the immediate sense of privacy and the fact that we are being recorded may go unnoticed, impacting our sense of privacy. Moreover, the knowledge that is built up from such data

[440] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit. p. 6; BREY, P. "Ethical aspects of facial recognition systems...", cit. p. 105.

[441] LÓPEZ ORTEGA, J.J. "La protección de la intimidad en la investigación penal...", cit., p. 304.

[442] For this opinion, see HIRANANDANI, V. "Privacy and security in the digital age...", cit., p. 1099.

[443] ARCHARD, D. "The value of privacy...", cit., pp. 24-25. The author states that the main concern of those who do not agree with the implementation of this technique is not the existence of CCTV as such, but its link with programs that allow facial recognition, among other issues. In spite of this, he concludes by pointing out that the concern is not the personal information but the use to which it is put.

[444] MARSHALL, S. "Private lives and public rules", in Claes, E. et al. (Dirs.), *Privacy and the Criminal Law*, Intersentia, Antwerpen, 2006, pp. 38-39. The author considers that the main problem deriving from the above perspective is that it is based on an oversimplified notion of what constitutes the public sphere and its relation to private life.

is capable of influencing the decisions that are made, even if one is not fully aware of it[445].

Case law has also taken a position on the issue of the expectation of privacy in the public environment or activities in which one interacts with others, which transcends the strictly private sphere and is linked to the right to a "social private life". The ECHR in various pronouncements has considered that the collection and storage of data by the authorities in such activities interfere with this right, such as participation in demonstrations[446] and others such as professional activities or those carried out in a public context[447], commercial and business[448]. Along similar lines, in the ECHR *Case López Ribalda and others v. Spain*, the applicants were dismissed as a result of recordings made with video surveillance systems in the workplace. It is debated whether the above-mentioned expectation of privacy exists in this context. The Court understands that a supermarket is a place open to the public and that the activities recorded there are not of an intimate or private nature, so that the expectation of privacy is limited. However, it goes on to argue that, even in public places, the creation of systematic and permanent recordings of images of identified individuals and their subsequent processing may raise issues affecting the privacy of those concerned. According to Spanish domestic legislation, those responsible for the systems have to give prior information to the individuals monitored by them. For this reason, since the applicant knew that they were being used and were fully visible, they have a reduced expectation of privacy[449].

Thus, some essential elements must be taken into account to consider whether the right to privacy is affected when an individual is away from home by the adoption or implementation of instruments capable of recording and processing images. In the event that individuals, either consciously or intentionally, perform some activity that can be recorded or communicated publicly and are aware of it, the expectation of privacy is reduced. The same is not true for data processing that results in the creation of material in the public domain, which extends to files collected by security services on a private individual.

There is no doubt that the individual has a right to individual privacy in relation to his or her own information even in the public sphere, but large-scale technological

[445] HILDEBRANDT, M. "Privacy and Identity", in Claes, E. et al. *Privacy and the Criminal Law*, Intersentia, Antwerpen, 2006, p. 43.

[446] Judgements ECHR *Case of Association "21 December 1989" and others v. Romania* May 24 2011, no. 33810/07; *Case Catt v. United Kingdom* January 24 2019, nº. 43514/15.

[447] ECHR Judgment, *Case Altay v. Turkey*, April 9 2019, nº. 11236/09.

[448] See, among others, ECHR Judgment *Amann v. Switzerland*, February 16 2000, nº. 27798/95.

[449] Judgment ECHR *Case López Ribalda and others v. Spain*, October 17 2019, nº. 1874/123 & 8567/13.

In the opposite direction, NORTH-SAMARDZIC, A. "Biometric technology and ethics...", cit., p. 444. The author argues that the use of biometrics in the workplace presents more problems than benefits, since privacy is violated in many of its aspects and anonymity cannot be preserved, consent is restricted by the imbalance of power, and the technologies present biases that can facilitate discriminatory decision-making. All these problems will be dealt with in greater depth in the following, but with reference to the field of law enforcement.

surveillance, including that exercised through FRs, can transcend this right and cause individuals to become targets of surveillance in almost every aspect of their lives[450]. Thus, surveillance operations, overt or covert, whether conducted by humans or machines, are intrusions that have a significant potential to disrupt privacy and thus dignity[451].

1.2.4. The right to privacy as a limit to state power

That the State can use biometric techniques for remote recognition of individuals considerably increases its surveillance potential and this undermines the ability of individuals to go about their lives unobserved, having a considerable impact on the exercise of the rights to freedom of expression, peaceful assembly, association and freedom of movement[452] (as will be discussed in more detail below in the corresponding section of this research).

As mentioned above, citizens have a personal need for privacy as an expectation that those in power will not interfere in certain areas of their lives that are considered private[453], which also extends to the public sphere. The latter is not understood as a single entity since it is made up of a whole complex of interconnected relationships, activities and physical spaces. As MARSHALL exemplifies, when one walks through a park, one is engaged in a public activity because others can see me and recognize me. The difference at this point lies in being simply seen or, also, the object of observation[454]. The latter is obviously disproportionate and inadmissible. However, he qualifies his position when he argues that observation, in the case of crime prevention, is not directed at the particular individual but at potential criminals, again finding the issue problematic when insidious surveillance is executed whose purpose is to watch all individuals as if they were potential criminals[455].

In this regard, it should be emphasized that the right to privacy serves primarily as a limit to the abuses of state power to curb the overreach of governments and their agents[456], but its intrusion is justified in certain circumstances such as in the prosecution of serious crimes and in case of terrorist threat, as it is considered a powerful tool to ensure security[457]. In this sense, MARCUS/MILLER argue that the right to privacy is nullified in a space that is monitored by CCTV to detect and stop crime and if the resulting

---

[450] NISSENBAUM, H. "protecting privacy in an inforamtion age...", cit., p. 179.

[451] MARSHALL, J. *Personal Freedom through Human Rights Law...*, cit., p. 76.

[452] HUMAN RIGHTS COUNCIL, *The right to privacy in the digital age...*, cit., p, 8.

[453] RENGEL, A. *Privacy in the 21st Century...*, cit., p. 30.

[454] MARSHALL, S. "Private lives and public rules...", cit., pp. 39-40. Similarly, SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics...*, cit., p. 30. The latter argue that a person does not have the right not to be seen when in a public space but does have the right not to be photographed.

[455] MARSHALL, S. "Private lives and public rules...", cit. p. 40.

[456] ARCHARD, D. "The value of privacy...", cit., p. 14.

[457] MEDEN, B. et al. "Privacy-Enhancing Face Biometrics: A comprehensive Survey," *IEEE Transactions on Information Forensics and Security*, vol. 16, 2021, p. 4147.

images are available only to the police for the sole purpose of identifying in a given area those who have committed the crime. Moreover, they consider it "morally acceptable" to use FR biometric systems to link the images collected by CCTV with the identity of those individuals who are included in a database[458] . However, for the limitation of this right to be legitimate, the principles of necessity and proportionality must be observed[459] as well as other requirements such as the existence of a solid legal basis[460], as we will have the opportunity to explain in more detail below.

Similarly, the *Case R (Bridges) v CCSWP and SSHD* judgment concludes that the South Wales Police's use of FRs in public places at the two times complained of by the applicant[461] was balanced and not disproportionate. The case in question stems from the complaint against the police for the use of FRs in public places at two different times and

[458] SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics...*, cit., p. 31.

[459] *Ibd*., p. 32.

[460] MARSHALL, J. *Personal Freedom through Human Rights Law...*, cit., p. 79.

Along these lines, see the ECHR *Case of Centrum För Rättvisa v. Sweden*, 25 May 2021, nº. 35252/08, for a case in which it was decided whether the Swedish government had made disproportionate use of new surveillance systems. Particularly in the case of secret surveillance, the risks of arbitrariness are obvious. It is therefore necessary to adopt specific measures detailing the rules for their use. In the case under analysis, the Chamber noted that the installation of this type of mechanism had a domestic law basis and was justified by national security interests. It went on to state that, given the current threats of global terrorism and serious cross-border crimes, as well as the increasing sophistication of communication technologies, the Court granted Sweden a wide margin of discretion to decide on the establishment of a mass interception of communications system. However, state discretion to implement such systems was more limited and the Court had to be satisfied that adequate and effective safeguards against abuse were in place. The regulatory framework had been revised on multiple occasions in order to protect privacy, thus minimizing the risk of interference with this right. More specifically, the purpose of intercepting and processing data was clearly defined in the Law, the duration of the measures was regulated, among other issues. Finally, it was noted that the Swedish system of signals intelligence provided adequate safeguards against arbitrariness and the risk of abuse.

The creation of a legal basis for regulating the use of FRs by police forces is favouring an authoritarian surveillance mechanism that does not guarantee rights and, on the contrary, allows a regime in which the level of control over our lives by the State and private companies increases. By allowing this technique, the State demonstrates an attitude towards the protection of rights in favour of increased state control, neglecting our security. Of this opinion, COUCHMAN, H. "Mass Surveillance on Our Streets...", cit., p. 589.

[461] The first took place on December 21, 2017 on Queen Street in downtown Cardiff. The time of operation was from 8:00 am to 4:00 pm. The purposes were to locate and detain "priority and prolific offenders". Three lists were used for this deployment: a) "net" comprising one person suspected of having committed a felony; b) "amber" with 382 individuals who had a warrant for their arrest; and c) "dwelling" with 536 suspects. There were 10 possible matches during use, 2 of which were erroneous. In one of the latter there was no intervention and of the remaining 2 ended in arrest. The plaintiff was present on this street at the time the system was being used and alleges that he did not see any warning signs.

The second time was on March 27, 2018. In this instance the FRs were deployed because in previous years at the Defence Exhibition at the Motorpoint Arena in Cardiff there had been disorder and those involved had caused damage and issued two bomb alerts that had disrupted the event. The time during which it was in operation was from 8:30 a.m. to 4:00 p.m. with cameras monitoring the entrance only. As above, there were three types of lists: a) "net" with individuals of interest who had been arrested the previous year at the same event, five of them for various offenses; b) "amber" with 347 people with warrants; and c) "dwell" containing 161 suspects. There were no arrests but no false alerts and correct identification. The plaintiff attended a demonstration that was held outside the venue where the event was taking place and was between 25-30 meters away from the FRs. He claims that he was not aware of their use and that the officers had not informed him in any way.

It could not be ascertained whether his data were captured by the instruments and, if they were, they would be deleted immediately because he was not on any list.

places. In that regard, the claimant alleges that it is a type of excessive and surreptitious surveillance to which he had not consented and, in fact, did not know that it was being used, thus being able to capture his biometric data and process it in an invasive way and, therefore, infringing his right to privacy. However, the High Court of Justice, analysing the characteristics of the specific case and not the consequences that FRs have in general or in the future (closer to dystopian societies such as *1984* or *The Capture*), considers that this was not the case. Among other reasons, for the fact that the instrument was deployed in an open and transparent manner, and with significant public participation. At each time, it was used for a specific and time-limited purpose, such as the selective search for individuals in a given area, just as the recordings were limited. Moreover, in both cases it served its intended purpose, as in the first case it resulted in the arrest of two individuals and, in the second, it identified a subject who had issued a bomb threat the previous year at the same event and had been taken into custody. On the other hand, no one was wrongfully arrested. In addition, no personal information was collected or retained from the applicant (to the best of our knowledge). For all of the above, it is concluded that there was no violation of the right to privacy[462].

On the contrary, the ECHR *Case of Glukhin v. Russia*. The case in question arose from the police identification of a man who held a peaceful demonstration alone, using a banner depicting a well-known activist. His biometric information was extracted from images and videos obtained from the social network Telegram and he was identified days later in the Moscow subway, which had CCTV equipped with FRs[463]. The Government admitted that the individual had committed an administrative infraction but never a crime. In this country, the use of FRs is foreseen in case of "necessity in a democratic society", extending this supposed necessity to this specific case, which is clearly disproportionate[464]. To this must be added the way in which the data has been collected and used, from social networks without the knowledge or consent of the owner; moreover, the Russian police did not inform at any time that they were making use of the FR technology. Therefore, it is concluded that there has been a violation of the right to privacy under art. 8.1 of the Convention.

[462] For his part, the individual claims that he did not know that the police were using such mechanisms, which is why he could not have consented to the collection and processing of his personal data. Thus, if this had taken place, his right to privacy would have been violated.

[463] The use of FRs has grown exponentially in a very short time in Moscow. In May 2017 there were only 3,500 CCTVs installed. In September of the same year, 3,000 were equipped with live FRs. In the spring of the following year some were installed in the metro. By September 2020 all CCTVs in Moscow (about 175,000) had FRs, being more than 220,000 in 2022.

[464] In this sense, ZALNIERIUTE considers that the Court could have explicitly validated the use of FRs in public spaces when necessary for the police investigation of what are considered the most serious crimes. ZALNIERIUTE, M. "Glukhin v. Russia. App. NO. 11519/20. Judgment," *American Journal of International Law*, vol. 117, nº. 4, 2023, p. 699.

In the ECHR judgment *Case S. and Marper v. The United Kingdom*, it is noted that the condition of necessity in a democratic society gives States a wide margin of appreciation on the decision to implement data retention systems relating to private life.

As will be discussed in greater detail below when addressing the principles by which the exercise of rights may be limited, any restriction on the content of the right to privacy depends on the factors of the case, including the seriousness of the circumstances of the particular situation and its consequences. Therefore, its use is disproportionate in minor offenses and, even more so, in mere administrative offenses such as the one just described. Nevertheless, in situations in which a danger or threat to public safety is observed, the use of FRs could be legitimized both in real time and delayed, since it is one of the exceptions established in the AIA to allow their use in the field of law enforcement. However, if we were to accept this situation, there would be a danger that its use would be expanded to other situations for which it had not been foreseen and which are not sufficiently intense to justify it. In such a case, a disproportionate use would be made of such instruments, regardless of whether they perform the identification in real time or delayed.

We must not forget, as noted above, that the FRs significantly reduce the ability of individuals to remain anonymous[465] and this represents a clear erosion of privacy, from the moment in which indiscriminately allows the scanning and examination of the identity of each person in a given range using their most sensitive personal data[466]. The intrusions to privacy are greater when the system performs a wrong identification and the individual who intends to go about his life normally is stopped in an invasive way by the police without any reason to do so.

In certain complex situations, such as the threat of a terrorist attack or the search for dangerous criminals or missing persons, society could legitimize the use of FRs, even though it is aware of the intrusion on the right to privacy that this entails. This was the case after the COVID-19 pandemic and the public health field, as individuals were more willing to accept state intrusions into their private lives to combat disease. Thus, health was seen as a powerful justification for some controversial measures. In that sense, some governments such as China knew where their citizens were, the places they had recently frequented and the people they had met[467]. Another example is South Korea, where a system was developed that combined FR technology with other technologies such as temperature scanning and identification of non-mask wearers[468]. As in the case of health, the same can happen with security, which carries the risk of granting an excessively high

[465] NAKAR, S. & GREENBAUM, D. "Now you see me. Now you still do...", cit., p. 109. The authors point out that this occurs even if measures are taken because the network of surveillance cameras equipped with this system is very extensive, in addition to the images and other information extracted from social networks. On this right in the public sphere and the involvement of the FRs in it, they discuss in greater depth on pages 114-116 of the same research.

[466] Similarly, COUCHMAN, H. "Mass Surveillance on Our Streets...", cit. p. 586.

[467] RAPOSO, V.L. "Health, privacy and liberty...", cit., p. 532.

[468] BURT, C. "Facial recognition temperature scanning, wearables and voice biometrics deployed for COVID-10 spread prevention", *Biometric update*, 3 August 2020. Electronic resource obtained via the World Wide Web: https://www.biometricupdate.com/202008/facial-recognition-temperature-scanning-wearables-and-voice-biometrics-deployed-for-covid-19-spread-prevention, [retrieved on 15 August 2024].

level of surveillance power to the State that could be maintained once the dangerous situation has passed.

Granting this privilege is dangerous because we are offering part of our private life to institutions and private entities that can use the information available to them to carry out massive surveillance of the citizenry, thus causing a feeling of constant surveillance and the consequent modification of our lifestyle and limitation of the exercise of fundamental rights and freedoms, which is known as chilling effects[469]. This process reaches all the rights involved, which are simultaneously affected by the impact that surveillance has on them[470], not only individual rights but also those exercised at the social level, affecting the effective functioning of participatory democracy, since this depends on the existence of an informed citizenry capable of getting involved in the community with a wide range of ideas. Thus, this pernicious effect derived from the use of privacy-invasive surveillance systems may result in the possibility of people refraining from participating in activities considered controversial, running the risk of undermining democracy[471].

Thus, privacy is fundamental to guarantee the development of other rights because if people do not feel free to act in the public sphere or interact with others, the protection of their personality, their own identity and freedom of expression is compromised, with particular intensity in relation to participation in demonstrations as well as the rights of assembly and association. Therefore, the approach we have adopted is based on analysing all of them individually yet interconnected, in what MURRAY has called "compound human rights harm" as a means of encapsulating broader types of harm that impact on several rights simultaneously[472]. This is because the RBIS and, more specifically, the FRs, interfere with all the rights indicated and their consequences on them can be known more precisely from this global perspective. In relation to the latter, it should be noted that the problems that will be addressed in paragraph five of this section are largely linked to some of the rights indicated, such as bias and the prohibition of discrimination or privacy and mass surveillance with its consequent chilling effect.

[469] This expression refers to the modification of the behaviour of individuals due to fear of being subjected to surveillance, whether in the real or virtual realm. PENNEY, J.W. "Chilling effects: Online surveillance and Wikipedia use," *Berkeley Tech. LJ.* vol. 31, 2016, pp. 126-127; MURRAY, D. & FUSSEY, P. "Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data", *Israel Law Review*, vol. 52, nº. 1, 2019, pp. 43-44.

The EDPB is also concerned about this issue. See, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 2.0 ...*, cit., p. 6.

[470] COTINO HUESO, L. "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos...", cit., p. 359. The rights to privacy and freedom of expression and demonstration act together to protect social processes. They cannot exist or operate in isolation. It is therefore recognized that a sphere of anonymity is essential to be able to freely exercise the latter two and thus contribute to the shaping of one's own identity. MURRAY, D. "Facial recognition and the end of human rights...", cit. p. 150.

[471] MURRAY, D. & FUSSEY, P. "Bulk surveillance in the digital age...", cit. p. 44.

[472] MURRAY, D. "Facial recognition and the end of human rights...," cit., pp. 150-151.

Not only that, but also in the field of criminal law, when the FRs are used by the LEAs, especially in preventive matters, it can cause the violation of the principle of presumption of innocence, since anyone can be scanned by the mechanism even when they have no relation to the criminal field, becoming a potential suspect.

In this sense, we conclude the study of this section by following COUCHMAN, who argues that "there is a wide range of legitimate reasons for seeking to protect our anonymity and keep personal information private, and we should not have to change how we live our lives to protect ourselves from unwarranted surveillance"[473].

1.3.Data protection

As we discussed in Chapter I, AI is based on data. Moreover, the latter, together with algorithms, constitute one of its essential components. The proliferation of data in recent years and its availability have led to the rapid expansion of AIs. Data can be personal and non-personal. The former are the ones that form the basis of the right analysed here. Therefore, we will focus on the analysis of the former because the face, as indicated above, is a personal data, a particularly sensitive type of private information with which a natural person can be identified because it contains information about him or her.

Along these lines, it should be clarified that personal data and information are not the same thing, although we sometimes use them interchangeably in the broad sense of data. The latter is the source of the information and the latter, in turn, is found within the data or a set of data that can be extracted or inferred. Thus, information is the elaboration of the datum[474]. Thus, the face is a biometric data that contains personal information of individuals that makes them identifiable.

The right to the protection of personal data is defined as the right of the data subject to exercise control, even active control, over such data. This right extends from access to rectification[475]. It is expressly recognized in art. 8 of the Charter as one of the essential freedoms of the individual. For this reason, it is included in Title II on "freedoms". However, it is not explicitly included in the Convention, but its protection is usually linked to the right to privacy in its broadest sense. Along these lines, the United Nations Human Rights Council in the year 2021 highlighted that AI interferes in the private life of individuals by extending, intensifying or encouraging the consequences thereof, especially with regard to the collection and use of personal data[476].

[473] COUCHMAN, H. "Mass Surveillance on Our Streets...", cit. p. 587.
[474] FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?...*, cit., p. 79.
[475] *Ibd.*, p. 72.
[476] HUMAN RIGHTS COUNCIL, *The Right to Privacy in the Digital Age...*, cit., p. 4.

The retention and use of data by the police is one of the issues that has generated most interest and controversy[477], especially when using mechanisms such as FR. Particularly significant is the image of the face, since we are dealing with biometric and, therefore, personal data, which is recognized as being of a particularly sensitive nature. For this reason, FRs in the scope of application of the law in public places represent an interference in the protection of personal data[478] from the moment in which the individual has the right to control his image and the data concerning it. In this case, what happens is that an image of the individual, which may be a photograph or a video, is taken and stored in a database that is susceptible to automated processing by the police, and the individual loses control over his own personal information.

1.3.1. Distinction between the privacy and data protection rights

The right that is the object of analysis in this point is closely linked to the previous one[479], being even considered as a modern version of privacy[480], being also known as "digital privacy", insofar as the protection of personal data stands as a protector of privacy in today's information society[481]. This is because the individual has the right to control his own personal data, deciding whether to make them public or to keep them in a reserved area and, therefore, inaccessible to third parties, and can also decide whether or not he wants them to be processed by other people.

In this regard, the FRA states that both protect similar values such as the autonomy and human dignity of individuals, guaranteeing them a sphere in which they can freely develop their personality, thoughts and share their opinions. It goes on to point out that both are a prerequisite for the exercise of other rights such as freedom of thought,

[477] COGHLAN, N. "*Gaughran* [2015] UKSC 29 on police biometric data retention: Strasbourg unheard, Strasbourg unheeded", *European Human Rights Law Review*, nº. 21, 2016, p. 61.

[478] HERVERG, J. & VAN GYSEGHEM, J.M. "La protection des données à caractère personal en droit européen- Chronique de jurisprudence (2020)", *Journal Europeen des Droits de l'Homme*, nº. 1, 2021, p. 69.

[479] PLACCO, A.V. "La protection des données à caractère personal dans le cadre de la jurisprudence de la Cour de Justice de l'Union Euorpéenne relative aux droits fondamentaux", in Grosjean, A. (Dir.), *Enjeux européennes et mondiaux de la protection des données personnelles*, Larcier, Bruxelles, 2015, p. 50. See, Judgement in *Case R (Bridges) v CCSWP and SSHD* (already cited), para. 58.

Some authors consider that both rights are one and the same. Thus, for example, SPROKKEREEF, A. & HERT, P. "Biometrics, Privacy and Agency...", cit., pp. 89-90; ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., p. 217. The latter argues that the object of protection of personal data is not the data of individuals but their right not to have their privacy intruded upon.

[480] Thus, ARCHARD, when addressing the conceptualization of privacy, links it to personal information in the sense of limiting access to it. ARCHARD, D. "The value of privacy...", cit., pp. 16, 26. More authors position themselves in this line, among others, MARSHALL, J. *Personal Freedom through Human Rights Law...*, cit., p. 50; MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal...", cit., p. 114; & RAPOSO, V.L. "Health, privacy and liberty...", cit., p. 532.

[481] DOCKSEY, C. "Articles 7 and 8 of the EU Charter: Two distinct fundamental rights", in Grosjean, A. (Dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, Bruxelles, 2015, p. 71.

conscience and religion, expression and information, as well as freedom of assembly and association[482]. Case law also understands that data protection is linked to privacy, among others, in the ECHR judgment *Frâncu v. Roumanie*[483], in which the individual requests the protection of his private life especially with regard to his confidential medical data which constitute a type of personal data. The Court concludes that respect for the confidentiality of health-related information is essential to protect the privacy of patients and preserve their confidence in the medical system and health services in general.

Notwithstanding the above, the rights to privacy and to the protection of personal data are distinct although they are closely linked, at least as far as the protection of personal information is concerned. Therefore, neither covers all aspects of the other. Thus, the right to the protection of personal data cannot be equated with the right to privacy in the broad sense[484], also known as the right to reserve all aspects of private life, which extends to many areas other than personal data[485], such as the home and the family[486]. Personal data and their need for protection are one more aspect of this right, instrumental for the complete protection of privacy. Along the same lines, there is talk of "informational privacy"[487], as the main aspect of privacy in relation to biometrics, since it involves the processing of personal data and image[488]. This type of privacy implies the protection of exclusion from knowledge or manipulation of data by others, as well as control over the data when they have been shared or allowed to be manipulated by third parties[489] . Likewise, this is a parcel of sovereignty over the data that affects us that should allow a retaining wall against the technological possibility of ubiquitous monitoring and knowledge of all the steps of our life[490]. This informational privacy can be infringed by tools that use the body as an identifier[491], including the face.

In addition, it should be noted that the Charter distinguishes between the two by including them in separate articles. The protection of personal data in the eighth and

[482] FRA, *Facial recognition technology...*, cit., p. 23.

[483] Judgement ECHR Case *Frâncu v. Roumanie*, 13 January 2020, no. 69356/13. See also CJEU, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert, Opinion of Advocate General Sharpston*, 17 June 2010, para. 71.

[484] DE LA MATA BARRANCO, N.J. & BARIÑAS UBIÑA, D. "La protección penal de la vida privada en nuestro tiempo social...", cit., p. 48.

[485] NERONI REZENDE, I. *Surveillance risks in IOT applied to Smart cities...*, cit. p. 31.

[486] DOCKSEY, C. "Articles 7 and 8 of the EU Charter...", cit., p. 82.

[487] This right may be violated by the use of the body as an identification tool. SPROKKEREEF, A. & HERT, P. "Biometrics, Privacy and Agency...", cit. p. 92.

[488] NORTH-SAMARDZIC, A. "Biometric technology and ethics...", cit., pp. 439, 440. He adds to the above, three more types of privacy: a) decisional, understood as the right of the individual to make decisions about his life without undue interference; b) spatial privacy as a physical spatial right of the individual that cannot be violated without explicit consent; and c) intentional, considered as the right to prohibit or prevent further communication of observable events or exposed elements such as the publication of photographs.

[489] Thus, it covers all processing of information of identified or identifiable persons. *Ibd.*, p. 83; DE LA MATA BARRANCO, N.J. & BARIÑAS UBIÑA, D. "La protección penal de la vida privada en nuestro tiempo social...", cit., pp. 45-46.

[490] DE LA MATA BARRANCO, N.J. & BARIÑAS UBIÑA, D. "La protección penal de la vida privada en nuestro tiempo social...", cit., p. 47.

[491] SPROKKEREEF, A. & HERT, P. "Biometrics, Privacy and Agency...", cit. p. 92.

privacy in the seventh. For this reason, we analyse them independently, understanding that they refer to different issues even though we are aware that they are closely related.

FINOCCHIARO adopts this position when she states that the right to the protection of personal data must be considered distinct from the negative freedom not to suffer interference in one's private life, the pillar of the right to privacy, and constitutes, for its part, the basis of the positive freedom to exercise control over the flow of one's own information. The right of confidentiality is of jurisprudential creation and consists in the exclusion of others from knowledge of personal and family events. Unlike the protection of personal data, it has a negative content, consisting of not making public and keeping certain information confidential, rather than a positive content, linked to the exercise of control over the data. Thus, unlike the protection of personal data, the specific object of privacy is not information, whatever its nature, but matters of all kinds reserved to others[492]. For this reason, we are dealing with two rights that are closely connected but which, at the same time, present significant differences.

1.3.2. Circumstances that promote the necessary protection of personal data

Today, the rapid processes carried out in the field of electronic data processing, the advent of computers and new information technologies in general have made it possible to collect and process data more easily and in less time. This situation is leading to a trend towards massive electronic recording of data relating to the private lives of individuals and an use of their data that goes beyond the purposes initially envisaged[493]. The fact that the population has increasing access to devices that allow information to be captured, stored and shared has facilitated the distribution of biometric data online. Billions of images and videos are shared on social networks, which favours the creation of massive image collections that can be processed and analysed using sophisticated computer vision and biometric recognition techniques[494]. One of the characteristics of Big data is that the data cannot be manipulated and processed with traditional mechanisms or processes[495], since it is impossible to handle this huge amount of information without new data processing technologies.

[492] FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?...*, cit., p. 73.

[493] TASSONE, L. "La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme", in Grosjean, A. (Dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, Bruxelles, 2015, p. 53.

[494] MEDEN, B. et al. "Privacy-Enhancing Face Biometrics...", cit. p. 4147. Because of the common use of biometric data in many everyday objects, such as smartphones, KINDT posits that public acceptance of data storage and collection for a large number of diverse purposes, beyond crime, has increased. These personal uses of biometric data may result in the creation of large data collections, not only useful in the public but also in the private sphere. KINDT, J.E. "Having yes, using no?...", cit., pp. 523-524.

[495] COTINO HUESO, L. "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata*, nº. 24, 2017, p. 132. As ESCAJEDO SAN-EPIFANIO states, what makes the difference now is not the amount of data available, but the ability to

The fact that these are processed and treated by ICTs plunges us into a state of electronic surveillance in which respect for our personal data and privacy in general is seen as a challenge to be met in a democratic society. To this end, as TASSONE states, any sector in which personal data may be processed must be equipped with appropriate rules to limit as far as possible interference with this right[496].

The enormous volume of information generated has great commercial value and as a source of knowledge. The natural vocation of data is to embrace both identification and identity, being able to be used to arrive at the former or to reconstruct the latter; and, in the opinion of RAFFIOTA/BARONI, the usefulness of a given piece of data is to serve as an instrument for identifying the individual who is *a priori* in a weak position, exposed to the persuasion of digital techniques and AIs for data collection and analysis[497]. Particularly worrying issues in relation to this right arise when the latter are extracted from social networks in which images, videos and other content are shared from which personal and biometric information can be obtained and used to create databases for, among other purposes, profiling or police identification. Therefore, of all the fundamental rights that have undergone changes with technological advances, the protection of personal data is the one that has undergone the most transformations[498] and is one of those that is most threatened by the use of RBIS in the field we have been analysing, especially because of the possible drift towards a context of mass surveillance[499], so it deserves special protection.

In this sense, the EU has enacted complementary and interconnected regulations to guarantee it: AIA, Cybersecurity Act, GDPR and LED. The latter specifically in the area of compliance with the Act. This has created a comprehensive regulatory triangle for the protection of personal data that covers the different areas in which it can be harmed.

---

discriminate between that information, the one that is useful. ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., pp. 238-239.

For this reason, the term Big Data usually refers to the phenomenon involving large-scale data collection and processing. VAN EIJK, N. "Mass collection of data: failing typologies", in *Human rights challenges in the digital age: Judicial perspectives*, Council of Europe. European Court of Human Rights, Strasbourg, 2020, p. 167.

For more on it in the criminal justice field, see, MOFFAT, K.H. "Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates," *Theoretican Criminology*, vol. 23, nº. 4, 2019, pp. 453-470.

[496] TASSONE, L. "La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme...," cit., p. 53.

[497] RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità...", cit. pp. 368-370.

[498] DONATI, F. "Introduzione. Il percorso della ricerca", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, p. 29.

The digital transformation has revolutionized the meaning and scope of data protection, inserting it into a new ecosystem full of actors and mechanisms that are partly different from those of the material reality. The transition to this new dimension has made it more complex –sometimes impossible– to identify who are the subjects that would act in the field of data protection. This is made more difficult especially with the extension of AI. BASSINI, M. & POLLICINO, O. "Intelligenza artificiale e protezione dei dati personali", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 269-271.

[499] DOCKSEY, C. "Articles 7 and 8 of the EU Charter...", cit., p. 89.

This regulatory framework was necessary because it is only in an adequately secure digital context that the true protection of personal data, of identity, can be guaranteed[500]. For the purposes of our study, the key ones are the GDPR, LED and AIA.

We have already indicated that the face is a particularly sensitive biometric data whose processing and use in the public sphere for law enforcement purposes, due to its special characteristics, is highly controversial. Therefore, we will now study it in depth, addressing aspects related to its controversial implementation in CCTV, the databases from which the information is obtained and the requirements to be met by any processing of biometric data to limit the infringement of this right as established in the legal texts mentioned above.

1.3.3. Biometric face parameters in public places with law enforcement purposes and the data protection right

The use of FRs to determine a person's identity jeopardizes the right to the protection of personal data and, therefore, the regulations that protect it. In the past, identification was carried out by individuals. Other mechanisms were introduced to speed up this task (cards, passwords, etc.) and, nowadays, with new technological advances, it is carried out by means of algorithms that automatically process certain biometric parameters.

As explained above, the system operates at different times. In each of them, the right to the protection of personal data may be violated in different ways. Firstly, when facial information is collected and transformed into a template without the owner's knowledge or consent, as it could be in the owner's mind to refuse such processing and to want the information to remain hidden. This situation is especially controversial –as we will have the opportunity to develop in greater depth later on– in the case of data coming from social networks or other virtual places where the subject shares photographs or videos in which his or her face appears; and, secondly, when the face is identified by comparing the image extracted from CCTV or other devices with the templates collected in a watchlist. In the latter case, the problem arises when the image is captured in the public sphere, where the individual, although his expectations of privacy are limited and, in this case, that his personal data will go unnoticed, reasonably expects that they will not be captured for identification purposes. Along these lines, the mere conservation and storage of personal data by the LEAs, regardless of how they were obtained, directly

[500] RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità...", cit. pp. 371-372.

impacts the privacy of those affected, regardless of whether or not they are later used[501] and regardless of the meaning of the result[502].

NERONI REZENDE lists the aspects of FRs that may collide with data protection: 1) errors, because even if DL techniques are used, they are not infallible, which puts under pressure the general principles of fairness and accuracy of data processing; 2) statistical inaccuracy of the data used in the training that may lead to biases. Discriminatory implications arise from these, which may also stem from the intentional use by police officers, who may take advantage of this tool to monitor ethnic minorities or marginalized and oppressed communities; 3) risks related to data security. Since biometrics can uniquely identify individuals and contains personal data, the loss of such data can have irremediable consequences for the subjects. In addition, the tools can be quickly altered, i.e., through deep fakes; and 4) public authorities often use FR technologies in cooperation with private entities, which entails the risk of data being collected by the latter and made available to them for a lucrative purpose. Similarly, a function creep may occur, in the sense that the data may be used for purposes other than the initial ones[503].

To those mentioned above, we also add the massive collection of data as it is susceptible to violate this right from the moment in which, through the same, can be known issues pertaining to the private sphere of individuals whose data have been stored, such as living habits, places and people who frequent, etc.

In line with what has just been noted, the CJEU has ruled on whether the general and indiscriminate collection of data would entail a violation of the right to the protection of personal data. The Court reaches the conclusion in the Joined Cases C-203/15 and C-698/15 (albeit for electronic communications services in general and not for the FRs although it can be extrapolated to the same), that the retention of data of users of electronic communications services involves a serious interference with the protection of personal data, which can generate in those affected a feeling of constant surveillance[504]. Likewise, in the Judgment of 6 October 2020, Joined Case C-511, 512 and 520/18, *La Quadrature du net and others*, has specified as contrary to EU law and the Charter, the activities of generalized and undifferentiated collection and storage of personal data for reasons of national security.

A recent application of mass data collection and consequent use for surveillance purposes was for the 2024 Paris Olympic Games. In this case, *Law Nº. 2023-380 of 19 May 2023 relative aux Jeux Olimpiques et Paralympiques de 2024* provides as one of its measures the so-called "video protection" consisting of the algorithmic processing of images in real time for the purpose of detecting anomalous behaviour and notifying them

[501] COTINO HUESO, L. " Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos..." cit., p. 360.

[502] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 2.0 ...*, cit., p. 5.

[503] NERONI REZENDE, I. *Surveillance risks in IOT applied to Smart cities...*, cit., p. 205.

[504] CJEU Joined Cases C-203/15 and C-698/15, December 21 2016. ECLI:EU:C:2016:970.

in order to adopt the measures deemed necessary by the LEAs (art. 10.1). It goes on to point out in the fourth paragraph of this article that these devices do not use biometric identification systems, do not process data of this type and, of course, do not use any FR technique. Thus, they cannot make any connection with personal data. Despite the provisions of the aforementioned Law, we believe that the door is being opened to the use and processing of biometric data insofar as the collection of images and their processing through algorithms is precisely the way biometrics works and falls within the concept of biometrics (see Chapter I of this research). Moreover, information regarding the way an individual behaves is a type of biometric data. Moreover, if the systems deployed identify facial emotions to detect anomalous behaviours, we are dealing with a type of FRs that, although it does not identify the face in a crowd, allows detecting strange behaviours through certain emotions and affections expressed through that[505].

The French National Commission expressed its opposition to the use of such techniques, as they may lead to a massive processing of personal data; they do not constitute a simple technological development but a modification of the nature of video devices that may entail serious risks for individual and collective freedoms and the consequent risk of surveillance and analysis in public spaces[506]. Although it is specified in the Law that facial recognition is not being used expressly, it could be used, given that the French Police have already deployed it at major events. For example at the Nice Carnival in 2019. On the other hand, in the event that the provision of the Law is complied with and this technique is not actually used, other biometric parameters such as the way of behaving would be used to identify the identity of a subject[507], which also entails a serious danger to the right to the protection of personal data.

In addition to the above problems, the Law provides for the authorization of real-time analysis of the images captured by these devices not only during the period of the Olympic Games but also before and after (from the time of enactment of the Law until March 31, 2025). The events chosen for implementation are listed in the first paragraph of art. 10 and are all those of a sporting, recreational or cultural nature that are exposed to risks of terrorism or serious attacks on security due to the magnitude of their attendance

[505] NOVOKMET, A. et al. "Facial recognition technology in EU criminal justice...", cit., p. 550. In a different way, the EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., 10. In this case, it understands that the mere detection of faces by "smart" cameras does not necessarily constitute an FRs in itself. He goes on to indicate that, for example, emotion detection cannot be considered as a biometric system that processes categories of personal data because they are not intended to univocally identify a person, but his or her behaviour. In the case of France, we understand that it would be used to detect individuals engaging in suspicious behaviour in order to prevent the commission of crime. For this reason, it should be considered in the same way as a conventional FRs.

[506] Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024 (demande d'avis n° 22017438).

[507] This approach is not unanimous in the doctrine and there are authors who consider that it will be necessary to wait for the development of the Olympic Games to verify if the way of behaving allows the identification of a specific individual. CASTETS-RENARD, C. & TURCI, A. "'Caméras augmentées': un danger pour les libertés lors des Jeux Olimpiques et Paralimpiques et au-delà?", *Recueil Dalloz*, nº. 22, 2023, p. 1139.

or their special circumstances. Thus, it is not limited only to the Olympics and the surveillance can be extended to the places where the indicated events are held and in their surroundings, vehicles and public transport and on the roads that provide these services. In addition, the images used may be collected from surveillance systems or cameras installed on aircraft, including drones. This represents an excessive extension of the spatio-temporal scope of application of such surveillance systems.

On the other hand, as we highlighted above, one of the main issues that arise in relation to this right is the source from which the information is extracted, generating great concern when images from social networks are used for this purpose. For this reason, we will now deal with this aspect as it has serious repercussions on the protection of personal data.

1.3.4. Sources from which face information is extracted: what happens with images published on social networks?

The police databases used for the implementation of RBIS that use the face as a parameter for identification can come from official sources such as biometric images of ID cards or passports as well as databases of known offenders against whom there is a search and arrest warrant or an open judicial process; or they can also be extracted from social networks and other virtual resources by the private sector[508].

As an example, the FBI has long used the Next Generation Identification system database that integrates facial templates with other types of biometric data such as fingerprints and other intelligence. The FRs has the ability to search state driver's license databases and other repositories such as USA Visitor and Immigrant Status Indicator Technology which collects biometrics of all non-citizens accessing the USA[509]. Not only in the public sphere but also in the private sphere FRs have been used. The social network Facebook, for example, launched a facial recognition application that detected individuals' faces in shared images and allowed tagging photographs with users' names and linking the images to their pages. This function was removed because of the problems it entailed in the right to personal data protection, which is why the generated templates

[508] The FBI recognizes that its databases may be comprised of images from official sources or from the Internet or social networks and are collected from the private sector. PREST, E.M. *Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System*, Federal Bureau of Investigation, 2019, p. 8.

[509] Other agencies with access to the FRs search are Customs and Border Protection, Coast Guard, Citizenship and Immigration Services, the Department of State, Department of Defense, and Department of Justice as well as law enforcement and intelligence services. In addition, the U.S. Government on a case-by-case basis may offer access to image repositories to partner countries such as Australia, Canada, New Zealand, and the United Kingdom. SMITH, M. & MILLER, S. *Biometric identificaiton, Law and Ethics...*, cit. p. 27.

had to be deleted[510]. The Hamburg Commissioner for Data Protection and Freedom of Information stated that the social network had violated the GDPR with this function and requested that it deactivate it and delete all biometric data that had been stored without prior consent.

This is because the use and collection of personal data without permission entails serious problems in relation to personal data[511], which can be used for different purposes such as profiling. In this regard, we bring up the case of *Cambridge Analytica*, a company dedicated precisely to that purpose. In order to elaborate them, it extracted private information from the Facebook profiles of more than 50 million users without their consent, representing one of the largest leaks produced in social networks to date and intended to influence the behaviour of the electorate in the 2016 USA elections and in the Brexit campaign[512].

Specifically in relation to our field of study, Pakistan uses face recognition for forensic identification. For this purpose, images extracted from CCTV are linked to the national identity database (NADRA) which is linked to other databases containing other parameters such as fingerprints[513]. KAUSAR et al. consider that NADRA is not sufficient to perform identification, so social networks such as Facebook, Instagram or Twitter (among others) should be used and open access data should be used[514].

In our view, the use of this last source of information is problematic and may lead to problems linked to the right to data protection of users whose photographs have been used to train the systems[515]. Not only in this case, but they could also be inserted in databases in the hands of the LEAs when they are deploying the FRs in the search for criminals.

A controversial case involving private actors in the collection and creation of databases through social networks and other websites is that of Clearview AI. The USA company offers its FR service to public authorities in order to identify suspects in police

---

[510] PESENTI, J. *Facebook. Una actualización a nuestro uso del reconocimiento facial*, 2021. Electronic resource obtained via the World Wide Web: https://about.fb.com/ltam/news/2021/11/una-actualizacion-a-nuestro-uso-del-reconocimiento-facial/, [retrieved on July 18, 2024].

[511] HUMBLE, K.P. "International law, surveillance and the protection of privacy...", cit., p. 17. The author reaches this conclusion after analysing the Cambridge Analytica case.

[512] ROSENBERG, M. et al. "The Company That Exploited Millions of Facebook Users' Data," *The New York Times*, March 20, 2018. Electronic resource obtained via the Web: https://www.nytimes.com/es/2018/03/20/espanol/cambridge-analytica-facebook.html, [retrieved on 18 July, 2024]. The data *Cambridge Analytica* collected included details of users' identities, their friendships, and the posts to which they had reacted. Only a small proportion of users had agreed to disclose their information to third parties, so obviously the data protection rights of those who had not had their information disclosed had been breached.

[513] More broadly, KAUSAR, S. et al. "Comparative study of forensic recognition and fingerprint during crime scene investigation and the role of artificial intelligence tools in forensics," *Journal of Development and Social Sciences*, vol. 5, nº. 1, 2024, pp. 585-597.

[514] *Ibd.*, 594.

[515] COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit., pp. 128-129.

investigations as well as to private security companies[516]. It goes beyond traditional FR tools limited to images collected by the government as it combined this technology with a database containing three billion images posted on the Internet, collected with automated software[517], which represents a massive data collection. This technique is also known as "data scraping", prevalently performed in the business environment and understood as "a plethora of Internet-based data retrieval methodologies, used without permission of the data owner". It can be manual or automatic through ML processes[518].

The aforementioned practice violates the right to personal data protection, and some social networks such as Twitter have sued the company, demanding that they stop collecting images from their website and delete all stored data[519]. In the event that it is intended to be implemented in the EU, we wonder if it would have any place, in view of the existing legislation on data protection. In this regard, the Swedish police have already used this application and the Swedish Privacy Authority (IMY) started an investigation, in which it concluded that the police had indeed used it on several occasions, and that some employees had even used it without the necessary prior authorization. IMY noted that the police did not comply with its obligations as a data controller when using Clearview AI, as it had not implemented sufficient organizational measures to ensure and demonstrate that the processing was in compliance with the Act and did not carry out an impact assessment. As a result, the IMY imposed an administrative fine on the police, ordered it to provide additional information and training to its employees to prevent future processing of personal data in breach of data protection regulations and has a duty to

[516] SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics...*, cit., pp. 27-28.

In 2022 the company sold its technology to the Ukrainian government to identify people in the war, dead or alive. CLAYTON, J. "La controvertida tecnología que usa Ucrania para identificar a los muertos y enemigos en la guerra", *BBC News*, April 3, 2022. Electronic resource obtained via the Web: https://www.bbc.com/mundo/noticias-internacional-61096583, [retrieved on 18 July 2024].

It is a different matter if the databases are used for algorithm training, i.e., from the private sphere, and are not used for law enforcement purposes. In this case, their use would be regulated by the GDPR and not by the LED. In this regard, we bring up the MegaFace database, which has stored more than one million faces of about 700,000 individuals. Consent has no virtuality in this case, since this requirement can be replaced by the pursuit of another purpose, as is the case with research, in this particular case, in facial recognition and development of algorithms and their training to improve their effectiveness. To build this database, Yahoo images were collected, with the consent of whoever had taken the photograph or recorded the video in which the images of the face taken appeared to form the database, created under a Creative Commons license that allows the images to be reused. For more on the issue, see, JASSERAND, C. "Massive Facial Database and the GDPR...", cit. pp. 169-188.

[517] NERONI REZENDE, I. "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective", *New Journal of European Criminal Law*, vol. 11, no. 3, 2020, p. 376.

[518] CAMPBELL, F. "Data Scraping-Considering the Privacy Issues," *Fieldfisher*, 2019. Electronic resource obtained from World Wide Web: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues, [retrieved on July 18, 2024].

KINDT is concerned that LEAs increasingly have access to databases not originally created for law enforcement purposes, whether from the public or private sector. This is because this situation may lead to the next step being the creation of regulations that allow access to such databases. KINDT, J.E. "Having yes, using no...", cit., p. 528.

[519] BBC, *Twitter demands AI company stops 'collecting faces'*, 23 January 2020. Electronic resource obtained via the World Wide Web: https://www.bbc.com/news/technology-51220654, [retrieved on 18 July 2024].

inform data subjects whose data was disclosed to the application where confidentiality rules allow it. In addition, they have to delete the personal data it contains[520]. Therefore, we must conclude that its use in the Union is unwise and violates the protection of personal data.

As the company collects publicly available images in order to deliver them to LEAs, the question arises whether this practice is executed with a purely economic/commercial or law enforcement interest. As the company itself does not carry out law enforcement activities but, as we say, sells its products to them, it acts with a purely commercial interest. Thus, it cannot be considered as performing a delegated function under the terms set out in art. 3.7 b) LED, so it would fall within the regulatory scope of the GDPR[521]. Considering that the face is a special category of data, its processing has to be carried out in accordance with articles 9 GDPR and 10 LED.

At this point, the question immediately arises as to whether the fact that users post an image on their social network makes it manifestly public (which is one of the reasons why the processing of such data is permitted). Social networks do not normally allow scraping, so the company would be in breach of data protection. But even when the images have been published on a public social network, it cannot be understood that there is tacit consent of the subject to be used by third parties for other purposes. Accessing the content is lawful because the owner of the image is authorizing it but, what he is not consenting in any case is its disclosure or use by others, who will need express consent to do so. This follows from what is established in the Judgement of Spanish Constitutional Court (Second Chamber) 27/2020, of February 24, where it is also noted that the publication in a social network is not comparable to the capture of images in public places. To this we must add that virtual spaces are not understood as public in the AIA.

And, if the capture and use of images in open profiles on social networks is an interference in the protection of personal data, even more so when they are private, because the owner is restricting the circle of those who can access the content published, making the image private[522]. Thus, even if information about oneself is freely published

[520] EDPB. *Swedish DPA: Police unlawfully used facial recognition app*, February 12, 2021. Electronic resource obtained via the World Wide Web: https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en, [retrieved 21 July 2024].

[521] NERONI REZENDE, I. "Facial recognition in police hands: Assessing the 'Clearview case'...", cit., pp. 378.380. The author discusses the territorial scope in which the company should develop its activities.

[522] Similarly, *Ibd.*, pp. 380-381. For its part, the EDPB in *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 2.0...*, cit., p. 6, holds that the fact that the user has made an image public does not extend the publication of the biometric data it contains, which can be extracted from the photograph by means of technical instruments.

To the contrary is the WP29 in *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, November 29, 2017, p. 10. It argues that in cases where personal data has been published on a social network there is a clear intention to make it public and acceptance of certain data protection rules that provide that all partners of the provider, including law enforcement authorities, have access to it.

and shared in such virtual spaces, it does not mean that privacy is being disregarded[523]. This is due to the fact that the user has the right to keep his data hidden from others, so that if the social network or website is private, the information shared therein acquires such consideration, and his personal data cannot be collected or used by others, even if they have the technical knowledge to access it. Likewise, it is part of the private sphere of people's lives that cannot be violated and, in the event that those are public, as in real life, there is an expectation of privacy, not being able to take the images for database creation purposes when the social network does not have a privacy policy that allows it, since the owner has not consented to such treatment and may not know that their data are being used for such purposes and offered to police or private security agencies. To all of the above it should be added that the company collects images indiscriminately of people who are not involved in criminal proceedings, involving a massive collection of personal information that clearly violates the right to the protection of personal data.

The fact that it is useful or convenient for the police does not justify its implementation because, in case of accepting its deployment, it would be granting an unprecedented surveillance power to the police, resulting in serious harm to citizens. Therefore, such databases should not be used, indeed, the EDPB calls for a ban on the scraping technique so that officers cannot access databases with information collected on a large scale and in a discriminatory manner[524]. Not only that, but such prohibition is already contained in the AIA, specifically in recital 43, under the understanding that the creation of databases through the non-selective extraction of facial images through the Internet or CCTV aggravates the feeling of mass surveillance and can lead to serious violations of fundamental rights. Therefore, they would not have in our environment. However, a nationwide police facial database could be acceptable in case of serious crimes and provided it is subject to adequate accountability mechanisms[525]. Nevertheless, we have to be cautious as the processing and treatment of the face by the police, even in cases of serious crime, may interfere with the protection of personal data. Therefore, in the following we will discuss the way in which to carry out an adequate data processing and the protection of the bases in which they are inserted, taking into account the normative provisions.

[523] NORTH-SAMARDZIC, A. "Biometric technology and ethics...", cit., p. 440. As the author states, the sharing of personal information in such spaces does not mean that individuals are any less concerned or aware of their privacy.

[524] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 7.

[525] Of this opinion, SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics...*, cit. p. 32.

1.3.5. Combination of data protection and artificial intelligence regulatory provisions in the field of RBIS

At this point we must consider the different regulations that deal with the protection of personal data, both at a general level, concretized in the GDPR and Convention 108+ (of very similar content to the previous one but with a broader scope in terms of territorial extent[526]), and specific to the application of the Law, where the LED has virtuality. In addition to the above, the AIA regulating the implementation of the RBIS, which includes the FRs. Therefore, there is an overlapping of all of them in this case and it is not easy to combine their content, since they are rules with very different logics. On the one hand, the AIA does not directly establish guarantees for those affected, but rather obligations for the providers of the systems and the companies or entities that use them; and, on the other hand, the GDPR, Convention 108+ and the LED do develop a system of data protection guarantees. Therefore, the latter will have to be observed for what is not provided for in the former. We will now analyse how their GDPR provisions combine in the area of compliance with the Law.

As pointed out in the third section of the previous chapter, the AIA initially prohibits the real-time use of RBIS for law enforcement purposes, acting as a *lex specialis* with respect to the provisions of art. 10 LED. This interdiction is not effective in three situations in which, under certain circumstances, they can be developed under the provisions of the Regulation. As specified in recital 18 of the AIA, the use and processing will be possible only if they comply with the framework established therein, with no margin for the competent authorities to use such data in the cases established by the LED. On the other hand, all other RBIS, including those acting in real time but for purposes other than law enforcement, will be governed by the Directive and not by the AIA. This follows from recital 39 AIA, which specifies that any processing of biometric and personal data associated with the use of AIs for biometric identification must still comply with all the requirements deriving from articles 10 LED and 9 GDPR.

In the specific case of the application of the law, recital 94 expressly refers to the first, when it indicates that any processing of biometric data for this purpose must comply with the provisions of this clause and also respect the principles set out in art. 4.1 LED, i.e. that the processing must be lawful and fair, transparent, limited as to purpose, accuracy and the period of storage.

In view of the restrictive nature of the prohibition established in the Regulation, a wide use of RBIS is allowed. In the case of FRs, we believe that this is particularly

[526] Convention 108+ has been ratified by all 28 EU member states, the four states of the European Free Trade Association, all the countries of the Western Balkans, some neighbouring countries such as Armenia and Georgia, Turkey and several African and Latin American countries. See, the Explanatory Memorandum of Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on May 2018.

problematic and, given all the controversial issues surrounding them, some cities and states in the USA have decided to ban them when they have been in use for some time[527] or have postponed their implementation. Even in Europe, a general ban on the use of these systems has been requested[528]; and, specifically, the EDPB in 2023 demanded it for RBIS operating in public places[529]; and, in the specific case of Italy, the use of S.A.R.I. Real time was suspended until specific legislation was in place[530].

However, the EU has endeavoured to introduce such systems in disregard of the abolitionist trend and has gone further, regulating the application of these mechanisms that operate in real time in cases which, although they are intended to be restricted, give a wide margin of discretion to LEAs, while those that operate with a more or less extensive time delay are not subject to such prohibition and no limitations are imposed beyond the requirements to be observed by all systems considered high-risk and the provisions of recital 95 of the AIA. The latter states that they must be used in a proportionate and legitimate manner, when strictly necessary and, therefore, selectively in terms of persons, location and temporal scope and on a limited set of data. Therefore,

[527] These include San Francisco, Boston, Portland and Oregon. In this regard, see SANTAMARIA, K.Y. "Facial recognition technology and law enforcement: select constitutional considerations", *Congressional Research Service*, 2020, p. 3; & FINKLEA, K. et al. "Federal law enforcement use of facial recognition technology", *Congressional Reseach Service*, 2020, p. 1.

The implementation of FRs in Tampa generated a lot of debate between the detractors and defenders of the technique from the beginning in 2001. The former argued the privacy issue and the latter the security benefits. In this regard, the latter consider that the technique brings great benefits, especially in terms of crime reduction and minimal costs. Opponents, on the other hand, argue that the harm caused to privacy and other rights and freedoms is greater, so it should not be implemented. To this they add the problems related to the accuracy of the system, as it is not completely effective and can lead to erroneous detections. For further discussion of both positions, see BREY, P. "Ethical aspects of facial recognition systems in public places...", cit., pp. 101-103.

[528] Not only in the police context, but in any other context. EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence...*, cit., p. 13.

[529] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 7.

[530] This is because the Italian Data Protection Guarantor in 2021 considered that this type of data processing greatly interferes with the private life of the data subjects and, therefore, had to find justification in an adequate regulatory basis. It is an automated processing of data on a large scale, able to observe even those who are present at political and social demonstrations that are not the object of attention by the police forces, thus being potentially revealing sensitive personal data that are not the object of police attention. He goes on to point out that the impact assessment indicates that these data would be immediately cancelled, but already the identification of a person in a public place entails the biometric processing of all persons circulating in the monitored public space, in order to generate the models of all to confront them with those of the persons who are included in the list. Thus, the nature of the surveillance activity itself evolves from the one aimed at certain individuals to the possible universal surveillance with the objective of identifying certain subjects. It also held that any limitation of the right established in Art. 8 of the Convention could only be made when it was provided for by law and constituted a measure that, in a democratic society, was necessary for national security, public safety, the economic well-being of the country, the defence of order and the prevention of crime, the protection of health and morals, or the protection of rights and freedoms. GPDP, *Parere sul sistema Sari Real Time* [9575877], dated March 25, 2021.

This was not the position it had always maintained, given that in 2018, it was in favour of the use of the system, considering that the identification constitutes a simple aid to human action, in order to speed up the identification carried out by the police operator of a wanted individual, whose facial image is available, without prejudice to the need for the latter to intervene to verify the reliability of the results of the system. GPDP, *Sistema automatico di ricerca dell'identità di un volto* [9040256], dated 26 July 2018.

rather than prohibiting or limiting their deployment to the essentials, their broad use is being permitted[531].

In the three cases in which real-time RBIS can operate, prior authorization is required as an initial requirement, except in cases of duly justified urgency. Furthermore, its use must be limited to what is strictly necessary and the principles of necessity and proportionality must be observed, considering the location, the consequences of not using the system and the impact on the rights of those affected (see section three of the previous chapter for more details).

1.3.5.1.Regulation of bioemtric data processing

As we can see, AIA allows the deployment of RBIS in both delayed and real time. The latter, in case of searching for victims of crime, prevention of threats or terrorism, and the location or identification of individuals to carry out a criminal investigation, prosecution or enforcement of a sanction, it is necessary to address the data protection regime[532], since being systems that use personal data and, more specifically, biometric data, they are subject to it.

The processing of both the latter and of other data considered as personal data of a special nature –as mentioned above– is subject to the general data protection regime and, more specifically, to the provisions of art. 9 GDPR, the first paragraph of which expressly prohibits the processing of such data, except for the exceptions established in the second paragraph, such as the consent of the data subject or the necessity of the processing, among other matters, for reasons of public interest. Moreover, as such data are subject to automated processing, it will also be necessary to take into account the provisions of art. 22 of the same norm, which provides that data subjects have the right

[531] This is without taking into account that other RBIS, for example, those used by private security companies, are not subject to the prohibition regime, nor are identity verification or emotion detection systems.

[532] In our analysis, we will focus on the GDPR and the LED because addressing them on a case-by-case basis would be excessive and far beyond the scope of our study. However, we point out the EU regulations that would have to be taken into account, to collect, store and share biometric data. These include Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry-Exit System (EES); Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for returning illegally staying third-country nationals; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border controls, amending the Convention Implementing the Schengen Agreement and amending and repealing Regulation (EC) No. 1987/2006; Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC). No. 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU; Council Decision (EC) 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime; Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

not to be subject to decisions based solely on a processing of the style –including profiling– that produces legal effects or significantly affects him or her in a similar way.

As our study is limited to the use of the systems in police matters, the baseline of the processing will be arts. 10 and 11 LED (parallel to the previous ones but with a less rigorous approach). The former, unlike the ninth of the GDPR, does not prohibit but restricts the processing of biometric data when it is considered "strictly necessary" and appropriate safeguards for rights and freedoms are observed provided that: a) it is authorized by the law of the Union or Member State concerned; b) it is necessary for the protection of the vital interests of the data subject or another natural person; and c) the data subject has manifestly made the data public.

The second precept gives States the ability to prohibit decisions based solely on automated processing (and profiling) in the same terms as the GDPR, unless there is authorization by the Member State or the Union and appropriate measures are provided for the protection of the rights and freedoms of the data subject, at least as regards human intervention by the controller. When biometric data are used, appropriate measures must be taken to protect the rights and freedoms (art. 11.2 LED), and profiles may not be drawn up that lead to discrimination of individuals, as stated in the third paragraph of this article.

1.3.5.2.Consent, Strict necessity and essential public interest

We now turn to the different cases that make up the exceptions established in the GDPR and the LED so that biometrics can be used in the police field. First of all, art. 9.2.a) of the GDPR refers to "explicit consent to the processing of those personal data for one or more specified purposes", which is also expressly included in art. 8.2 of the Charter as one of the elements that guarantee the exercise of the right to the protection of personal data. Therefore, it continues to be one of the cornerstones of personal data protection[533] whose validity as a legal basis derives from a series of predicates that must be respected. Among them, the informed nature, as a presupposition that the expression of will of the data subject can legitimize the processing of data by the owner. Consent must be given when the data subject is duly informed, among other things, of the characteristics of the algorithmic system used[534]. Other aspects that must be present for it to be valid are that it

[533] MILOSSI, M. "Remote biometric identification systems and ethical challenges...", cit., p. 3; similarly, NORTH-SAMARDZIC, A. "Biometric technology and ethics...", cit., p. 441. Despite this, the latter argues that consent does not solve all ethical dilemmas related to privacy because, among other issues, they will not be able to offer it in case the mechanism is deployed in the field of surveillance and security.

[534] BASSINI, M. & POLLICINO, O. "Intelligenza artificiale e protezione dei dati personali...", cit., pp. 275-276. Thus, the data subject has to be aware of the operating modalities of an algorithmic processing.

is given expressly, specifically, and freely or fully consciously and not as a result of any conditioning factors[535].

The above would be for general data processing, but what happens when biometrics is intended to be used for law enforcement purposes? Article 8.2 of the Charter, when it refers to the need for consent, adds that the processing of personal data may be based either on consent or on any other legitimate basis provided for by law. It should be added that, from the wording of the AIA, the irrelevance of the data subject's consent seems to be inferred[536], at least with regard to the biometric identification referred to in the Regulation, i.e., that which acts in real time and is implemented by the LEAs, given that recital 15, when it establishes the concept of biometric identification, specifies that it involves the automated processing of human characteristics to determine the identity of an individual by comparing his biometric data with those stored in a reference database, regardless of whether he has given his consent.

Similarly, it is not included among the exceptions in art. 10 LED to allow the processing of data. Therefore, in the police field there is no such provision and, provided that the exceptional circumstances offered for in art. 13.3 LED occur, it will not be necessary (as with the right to information, with which it is closely linked), so we understand that it is irrelevant whether it exists or not, since, in many situations, the actions of the agents may be secret or covert, especially in cases of serious crimes and terrorism. In these cases, it is impossible for the subjects to whom it is addressed to consent to the biometric data of their face being processed, and it must be so, in order not to obstruct the investigation.

In our opinion, the consent of the individual subject to a search and arrest warrant for the commission of a serious crime or situations in which there is a real danger or threat of serious crime or terrorist attack is one thing, and the situation in which such circumstances do not exist is another. In the first case, consent would be irrelevant. As stated in art. 13.3 LED, there are situations in which States may decide not to provide information to the individual when necessary and proportionate, such as to avoid hindering investigations, to avoid prejudice to the prevention, detection, investigation or criminal prosecution; protection of public and national security, as well as to protect the rights and freedoms of citizens. However, it is quite another matter when such exceptional circumstances do not exist and the mechanisms are deployed. In this case, the data of individuals are collected in a database that can be used by the police at any time for

[535] These four requirements are established by European standards on the validity of consent. However, we must be aware that the one issued in the field of personal data protection is not the same as the one issued in the field of business, due to the specific circumstances of each particular field. RICCIO, G.M. & GIANNONE CODIGLIONE, G. "La rilevanza delle basi giuridiche per il trattamento di dati personali mediante sistemi di intelligenza artificiale", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 288-289.

[536] On the contrary, TORRE, M. "Nuove tecnologie e trattamento dei dati boimetrici nel proceso penale...", cit., p. 680.

investigative purposes or, being in a public place, are susceptible to be detected by the system and identified, even erroneously, with the serious consequences that this entails.

In the first case, consent –we reiterate– would be irrelevant, but not in the others, where it must be given in order for the processing to be lawful under the provisions of art. 6 GDPR. For such consent to be valid, it must be given by the data subject affirming or denying the processing once he or she has been duly informed and in a transparent manner, as will be explained in more detail below. This was the case in *R Bridges v CCSWP and SSHD* (cited above), where the data subject argued that he did not consent to the capture and processing of his personal data because he did not know that the area he was walking through was equipped with cameras furnished with the FR technique. On the other hand, the police argue that people were informed about this point because there were signs indicating it, which is why it is understood that the individual knew that FRs were being used and, therefore, if he decided to continue walking through this area, he would be giving his consent to a possible processing of his personal data, since if he is not one of the persons subject to identification, in principle, he should not be detected.

Linked to consent, we find the exception contained in arts. 10.c) LED and 9.2.e) GDPR, on the fact that the processing refers to "personal data that the data subject has manifestly made public". This issue ties in with what has already been explained above in relation to databases and the use of images taken from social networks for their constitution.

We reaffirm what we pointed out previously, in the sense that, on the one hand, the fact that images are published on social networks and other websites is not a sufficient argument to justify the processing of biometric data of an individual and their insertion in a database for police purposes for subsequent identification. This also applies in the case that the profile of the user who shares such content is public, as he or she expects that it will not be used for other purposes; and, on the other hand, when in a public space, even if it is equipped with surveillance cameras with the function of FR, it is not consenting to the face being captured by such devices. Therefore, this provision has no place to legitimize the processing of biometric data of the face of the subjects for police purposes. This would be regardless of whether the mechanisms act in real or delayed time or whether the data is deleted immediately, because even when it is recorded and deleted in a matter of milliseconds, the pedestrian is captured by the system and his data is checked against a search list. In addition, the possible subsequent use and retention of this processed data may more intensely affect the rights[537]. Let us not forget that we are processing personal data considered special whose use, as we can see, is very restricted.

Regarding the criterion of strict necessity, we agree with COTINO HUESO when he states that, even with legitimacy and quality legal regulation, these systems must be

[537] COTINO HUESO, L. "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", *El Cronista del Estado Social y Democrático de Derecho*, nº. 100, 2023, p. 71.

subject to strict scrutiny in terms of necessity, proportionality, adequacy or minimization, given the strong impact they have on society and on rights[538]. The more profound the interference in the latter, the greater must be the requirements of necessity and proportionality[539] and, as in this case the latter is excessive, if the aim is to implement a mechanism of this type, the aforementioned requirements should be expressly specified and very high. This follows from the provisions of art. 11.2 LED, given that, when the processing is automated, because it involves greater interference with rights and freedoms, the protection measures to be implemented must be higher[540]. The criteria of necessity and proportionality will be discussed further on, above, when the limits to fundamental rights are studied in greater detail.

Finally, the need to protect the vital interests of the data subject or another natural person (article 10(c) LED) could be found in the maintenance of public order and social peace that is disturbed by crime. In this sense, in the case of serious crimes or terrorist threats, its use could be justified because it seriously endangers public safety. It is in such terms that its development is foreseen as established in art. 5.h.ii) AIA for systems acting in real time. Likewise, the search for victims of certain crimes and missing persons is an essential interest (art. 5.h.i) AIA), as is the location of suspects of serious crimes (art. 5.h.iii) AIA) in order to bring them to justice for investigation or prosecution or the enforcement of a criminal sanction. However, allowing its deployment in these terms may result in its extension to other situations that are not so serious and therefore do not require it, using the argument of necessity for this purpose, as happened in the case of the ECHR *Glukhin v. Russia* judgment, as it was used for the imposition of a mere administrative sanction, which is not acceptable as it does not constitute an essential public interest, involving a disproportionate and excessive use by the police and, in no case, justified.

[538] COTINO HUESO, L. "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos...", cit., p. 383.

[539] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement...*, cit., p. 45.

[540] Regarding the requirements for the automated processing of personal data in police matters, it is very interesting what is contained in the Judgment of the First Chamber of the Federal Constitutional Court of Germany, dated February 16, 2023 (1 BvR 1547/19, 1 BvR 2634/20). It establishes different guiding principles to determine the greater or lesser intensity of the interference of automated data processing: consideration of the greater or lesser duration of the tracking, whether spatial or geographical tracking data are included, whether they result in personality profiling, whether information is obtained that serves as a starting point for other measures unrelated to those that motivated the initial intervention, whether there is automated recognition technology and whether there are specific risks of discrimination.

About the variable factors according to "the nature and scope of the data" it establishes some criteria related to the amount of data, the diversity of the data used together, the inherent relevance of the data, the origin of the data or if there is data from social networks. When obtained through surveillance in private homes or remote searches of computer systems, the requirements are even stricter.

Data analytics methods can affect the personalities of stakeholders, the impact is far greater when data and algorithmically calculated assumptions about the relationships and contexts of the affected individuals' environment are included. Automated enforcement can drastically change the way police work and can increase the weight of individual impairment. The intensity of the restriction becomes dependent on the methods of analysis or evaluation, when automated, it is more intensive in intervention if the knowledge obtained about the individuals is broader and deeper, being also greater the possible errors and discrimination and, much more complicated to understand the software.

1.3.6. Requirements on data processing and their storage in databases

The collection and processing of facial images must be carried out in strict compliance with European data protection regulations. Thus, it must comply with a series of requirements included in arts. 4 LED and 5 GDPR. In general, both establish the following[541]: a) lawful, fair and transparent; b) follow a specific, explicit and legitimate purpose; and c) comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability[542]. We will focus specifically on the provisions of the LED, since it is the one that is relevant to our study, as it regulates the police processing of biometric data.

The second paragraph of art. 4 LED allows the processing of personal data, by the same or another controller, for the purposes of prevention, investigation, detection or prosecution of criminal offences or their execution, including the protection and prevention of threats to public security (art. 1.1 LED), provided that: a) the controller is authorized to process such data for that purpose; and b) the processing is necessary and proportionate for that other purpose. In both cases, according to the law of the Union or Member State concerned. The processing may include archiving in the public interest, scientific, statistical or historical use, observing appropriate safeguards for rights and freedoms (art. 4.3 LED). At this point we will focus on the first three requirements, addressing those of necessity and proportionality, as already indicated, above.

1.3.6.1.Lawful, fair and transparent

The first element to be studied is the lawfulness of the processing, fairness and transparency. In this sense, in order to guarantee this, especially in the field of real-time facial recognition technologies, it is necessary to provide clear information to data subjects, given that images of individuals' faces are usually captured by cameras in public places without their knowledge or consent[543]. For that reason, the right to be informed is a prerequisite for the exercise of other rights, such as requesting access to stored data,

[541] Letter e) changes a little depending on the scope in which the processing occurs, as the GDPR states that the retention period shall be until the identification of data subjects is permitted and for no longer than is necessary for the purposes of the processing of personal data. However, as an exception, they may be kept longer when the data are processed only for archiving purposes in the public interest, scientific or historical research or statistical purposes, applying appropriate technical and organizational measures to protect the rights and freedoms of the data subject. For its part, the retention period provided for in the LED is limited to that which allows the identification of the individual and for no longer than is necessary for the purposes pursued.

[542] Art. 8.2 of the Charter takes up the above with the following wording: "Such 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 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".

In addition, on these requirements, see Articles 5 and 8 of Convention 108+.

[543] FRA, *Facial recognition technology...*, cit., p.24.

demanding its deletion or rectification and issuing a complaint to the supervisory authority and receiving an appropriate remedy[544].

However, this right is not absolute and recital 26 LED establishes as an exception covert investigations and video surveillance in the criminal field, on condition that it is provided for by law and is a necessary and proportionate measure in a democratic society, and the legitimate interests of the data subject must be respected. It goes on to point out the duty to inform individuals of the risks, rules, safeguards and rights applicable in relation to the processing of personal data and how to assert their rights in relation to such processing.

Articles 13 and 14 GDPR as well as 13 LED specify the content and form in which the information must be provided to the data subject. They specify that individuals have to be informed about the identity and contact details of the controller, the purpose of the data processing, the retention periods, the right to request access to the collected data[545], its deletion or rectification, as well as the right to complain to a supervisory authority[546]. However, art. 13.3 LED details a number of exceptions. Thus, States may adopt measures for delaying, limiting or omitting to make information available to the data subject when the measure is necessary and proportionate in a democratic society, taking into account in any case the fundamental rights of the individuals concerned.

These exceptions are specified as follows: a) to avoid hindering official or judicial inquiries, investigations or proceedings; b) to avoid prejudice to the prevention, detection, investigation or prosecution of criminal offenses or their execution; c) to protect public safety; d) to protect national security; e) to protect the rights and freedoms of others. In the case of the deployment of FRs in public places for law enforcement purposes, this right to information may be restricted, as well as the right to consent (closely linked to transparency and the right to information, insofar as, for an individual to be able to consent to the processing of his personal data, he must be provided with all the necessary information) in the case of the search for terrorists or suspected dangerous criminals. Limitations that, in any case, must be strongly justified[547] in order not to violate the rights and freedoms of citizens and to make responsible use of the mechanisms.

In the absence of the exceptions listed above, individuals have to be informed of the processing of their personal data and this, in the law enforcement environment, is complicated, which is why consent is not one of the legal bases for processing biometric data in the law enforcement environment, but it is true that certain information must be provided so that individuals are aware that their personal data may be captured and

[544] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 525.

[545] The bases of this right are specified in Art. 14 LED and the limitations thereof in Art. 15 LED, which coincide with the exceptional circumstances provided for in the third paragraph of Art. 13 LED to restrict the right of information.

[546] Articles 16 and 17 LED, respectively.

[547] FRA, *Facial recognition technology...*, cit., p. 24.

processed by a FRs. Such basic information includes the identity and contact details of the controller, the purpose of the data processing and the retention time[548].

The EDPB specifies the way in which the information has to be provided in order to comply with the transparency obligations, adopting a multi-layered approach and a combination of methods. In a first step, the most important information should be displayed by means of a warning sign at the place where the technique has been implemented, which may be accompanied by an icon providing an adequate overview of the data processing in an easily visible, intelligible and clearly legible form; the information should be provided in such a way that the data subject can easily recognize the circumstances of the surveillance before accessing the monitored area, where the location of the camera need not be disclosed if there is no doubt about the areas under surveillance and the context is clear. In addition, the data subject must be able to estimate the area that is subject to the measure in order to avoid surveillance or adapt his or her behaviour if necessary. The information provided at this first level must contain the most important information (i.e., purpose of the processing, identity of the data controller, the data subject's rights and the effects, among others[549]). The other data pertaining to the second level may be provided by other means that are easily accessible to the data subject, such as a comprehensive information sheet available at a central location[550].

Another way in which data can be made accessible and transparent is the requirement set out in arts. 51 and 71 AIA that the systems be registered in a public database. The EDPB-EDPS welcome this provision as they see it as an opportunity to provide information to society about the scope of the AI and the defects and incidents that may compromise its operation and the solutions adopted to remedy them[551].

The FRA argues that new technological developments and their data processing capabilities increase the level of intrusion on fundamental rights, because the extraction of biometric elements from a face makes it visible for processing in other ways, which increases the aforementioned intrusion. As a consequence, the availability of a facial image in a database is different from the application of software that extracts the parameters of the face in an automated way, regardless of whether or not the extracted features are compared with a watchlist[552]. For this reason, additional protection of the

[548] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 525.

[549] EDPB. *Guidelines 3/2019 on processing of personal data through video devices...*, cit., pp. 28-29.

[550] *Ibd.*, pp. 29-30.

[551] EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence...*, cit., p. 22.

[552] FRA, *Facial recognition technology...*, cit., p. 25.

Similarly, but in this case for DNA samples, the ECHR *Case S. and Marper v. The United Kingdom* concludes that the mere storage of DNA profiles constitutes an interference with the right to the protection of personal data because their automated processing allows the authorities to go beyond "neutral" identification. More paradoxically, it is the specific processing methods to which fingerprints are subjected that determine that their mere storage constitutes an interference with this right.

data subject's personal data is required, guaranteeing a lawful, fair and transparent use, providing all the necessary and appropriate information so that individuals know that their information is being processed and the purposes of such processing, so that they are able to give their consent or not and exercise their rights of access and, where appropriate, rectification or deletion.

In the police sphere, this requirement may be limited provided that certain circumstances are met, such as the secrecy of the proceedings[553]. However, this provision cannot be a *carte blanche* that legitimizes an excessive and unjustified limitation of the right to information and the other rights that go with it when processing personal data. Therefore, there must be a strong justification that legitimizes it.

Following RAPOSO, we state that the regulations governing FRs in the field of legal compliance must contain adequate measures to ensure compliance and its requirements, among which is the rule of law. The two cornerstones of compliance are transparency and public scrutiny and, to achieve this, strict control of the algorithms used and a record of how they are programmed, as well as the data and methods that were used for training, are required. Regulations should clearly establish the responsibility of LEAs when using FRs and citizens have the right to request respect for due process and the rule of law, including proportionality, transparency and guarantee of adequate compensation in case of suffering any harm[554].

Thus, all the above aspects must be reflected in the legislation that covers the use of FRs. This is because the mere fact that the use of biometric systems is contained in a regulation does not necessarily imply that it is constitutional or respects the rights of the individuals concerned[555]. Therefore, if it is intended to implement FR mechanisms, the way in which this is to be done must be clearly detailed, taking into account all the

[553] In such cases, appropriate safeguards must be established and the IAs must be registered and provide transparency, not only to the public, but also to the competent supervisory authority. EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence*..., cit. p. 22.

[554] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., pp. 526-527. The author points out that, from a privacy perspective, a Data Protection Impact Assessment (Recitals 53 and 58 and Art. 27 LED) and a consultation of the supervisory authority (Recital 96 and Art. 28 LED) should be carried out. Likewise, a mechanism for checking and balancing the use of FRs should be developed. On the other hand, an authorization from the independent judicial or administrative authority is required based on the criteria of proportionality and necessity according to the objectives pursued.

ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit., pp. 6-7. The authors point out that safeguards and measures addressing risks to the rights of individuals in the design of biometric systems and the processing of these data should be based on the Data Protection Impact Assessment and, if during this process it is found that high risks remain, the national supervisory authority should be consulted. Measures and safeguards to avoid system risks should be adopted in the design and subsequent implementation of the mechanism, ensuring data protection by design and by default.

Not only in the EU, but also in other countries such as the United States, such evaluations have to be performed. In fact, the FBI is obliged to do so in its FR technology. NAKAR, S. & GREENBAUM, D. "Now you see me. Now you still do...", cit., p. 106.

[555] MITCHELL, A. "Distinguishing friend from foe...", cit., p. 315.

appropriate legal guarantees, as well as the limits of its use, considering the respect of all the rights and freedoms involved.

1.3.6.2.Specific, explicit and legitimate purpose

The collection of images by an FRs must be done for a defined and limited purpose[556]. This, together with the interest served by such purpose when compared to those of the data subject, is one of the criteria to be applied when processing data without the data subject's consent.

It is provided for in recital 26 LED, which also states that it must be determined at the time of collection of personal information. Thus, the images must be obtained for specified, explicit and legitimate purposes and not be processed in a way that is incompatible with those purposes (art. 4.1.b) LED). Art. 5.4.b) of Convention 108+ adds that further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes is compatible with those purposes if it is carried out subject to appropriate safeguards (without specifying which ones).

This principle could be linked to the maintenance of national security, public safety or the economic well-being of a country, the prevention of crime and disorder, the protection of health or morals, and the protection of the rights and freedoms of others[557]. The ECHR has ruled on the right enshrined in art. 8 of the Convention on several occasions when personal data are collected and processed in criminal matters, concluding that it can be limited for this purpose but providing guarantees for it, such as the fact that it must be enshrined in a law. Thus, in the Judgement in *Case Friedl v. Austria*, it considers that the aforementioned right is not violated because the interference in the private life of an individual can be considered necessary in a democratic society where this limitation has been produced to fight crime. Similarly, in the Judgement in *Case Leander v. Sweden*, the Court held that the government of Sweden could consider that national security interests prevailed over the individual interests of the applicant and, therefore, it was allowed to collect his personal data. In *Case Klass and others v. Germany*, the Court concluded that the interception of communications by the police and security services is an interference with this right but necessary in a democratic society

[556] Purpose limitation is one of the fundamental principles of the right to the protection of personal data, as highlighted by the A29 WP in *Opinion 03/2013 on Purpose Limitation*, WP 2013, 00569/13/EN, Brussels, 2 April 2013. Thus, the use of the systems has to be proportionate in relation to the legitimate purpose pursued. EUROPE COUNCIL. *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*..., cit. p. 12.

Biometric data is sensitive data, so it must be secured and used for a specific purpose, especially in the field of law enforcement. ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit. p. 9.

[557] FRA, *Handbook on European data protection law, 2018 Edition*, Publication Office of the European Union, Luxembourg, 2019, p. 45.

and should therefore be provided for in a law[558]. Thus, in *Case S. and Marper v. The United Kingdom*, the Court held that the collection and maintenance of biometric data, in this case, fingerprints, DNA and cellular samples, fulfils a legitimate purpose established in the law of the United Kingdom where it is foreseen that these samples can be taken and kept permanently after the commission of the crime. Therefore, the Court does not understand that the protection of personal data has been affected as claimed by the applicants as their use and maintenance is based on relevant and sufficient reasons. Moreover, they are used for the broader purpose of identifying future crimes, thereby also preventing delinquency.

Specifically in the area of video surveillance, we find the ECHR Judgement *Case Peck v. The United Kingdom*, which relates to an incident in which the applicant attempted suicide in an area where a CCTV was recording and was not aware of it. The police observed what happened and prevented him from continuing with his suicide plan[559]. In this case, a vital interest of the data subject, such as his life, was being safeguarded, which is why the processing of personal data was legitimate. Similarly, in *Case Gardel v. France*, the registration of the applicant's personal data in the national automated judicial database of sexual offenders was not contrary to art. 8 of the Convention.

Legitimate objectives must observe three requirements for purpose specification, defined by the A29 WP in 2013, namely that the data be:

a) Precise: the purpose must be sufficiently defined to allow the implementation of the necessary safeguards to ensure data protection and to delimit the scope of the processing;
b) Explicit: the purpose must be unequivocal and clearly expressed so that there are no difficulties in understanding;
c) Legitimate: duty to respect applicable legal and ethical provisions[560].

[558] ECHR *Case Klass and others v. Germany*, 6 September 1978, no. 5029/71. In this pronouncement, the Court held that the legislation on secret surveillance of postal and telephone communication channels must be subject to restrictive conditions established by law to guarantee the protection of rights. Similarly, in the *Malone v. The United Kingdom case*, the Court concluded that the interception of communications in the course of a criminal investigation, as well as the interception of a telephone conversation, is an interference with Art. 8 of the Convention. The law must use clear terms to sufficiently indicate to everyone under what circumstances and on what conditions it enables the implementation of secret and potentially dangerous violations of this right. Since the implementation of measures to monitor secret communications is beyond the control of the interested parties and the public, the law would be contrary to the rule of law if the state's discretion were not limited.

On the other hand, in *Case P.G and J.H. v. The United Kingdom*, 25 September 2001, Nº. 44787/98, the Court concluded that the right to privacy was violated because the law did not provide for the recording of the plaintiffs' voices.

Many other decisions along these lines can be consulted in TASSONE, L. "La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme...", cit., pp. 60-64.

[559] Judgement ECHR *Case Peck v. The United Kingdom*, nº. 44647/98, 28 January 2003.

[560] A29 WP, *Opinion 03/2013 on Purpose Limitation*..., cit. The Opinion further recognizes that the principle of processing limitation is one of the essential keys to data protection and aims to strengthen its protection while recognizing that its application should not be too rigid.

With regard to our object of study, when it comes to real-time RBIS, the AIA establishes three exceptional situations in which the prohibition is not applicable and, therefore, they can be used because it is provided for in the Regulation. This is not the case with the mechanisms that act in delayed mode, leaving a wide margin of discretion to the agents to decide when to implement them, given that the only thing that recital 95 of the AIA states is that the use of such instruments will be subject to guarantees –without detailing which ones– and that it will be done in a proportionate and legitimate manner, when strictly necessary and selective according to the persons to be identified, location and temporal scope and making use of a limited set of legally obtained recording data. It goes on to state that they must not be used in such a way as to result in indiscriminate surveillance or to circumvent the conditions of prohibition and strict exceptions to which real-time systems are subject.

As can be seen, despite the insidiousness of the technique, the requirements are much laxer, which gives the agents a very broad decision-making capacity and this is not in line with the provisions of the regulations on personal data protection, so that a disproportionate use can be made of the RBIS in deferred, seriously endangering, if not violating, not only this fundamental right but all the others. With greater intensity when the biometric information handled is that of the face by means of FRs.

Along the same lines, as pointed out by the FRA, the purpose of facial image processing by this instrument should be strictly limited to the fight against terrorism and other forms of serious crime (including serious threats of such crimes[561]), as this is the delimitation made by the EU law for law enforcement access to large-scale databases. Likewise, it could be extended to the purpose of identifying missing persons and victims[562]. These are essentially the purposes set out in the AIA for real-time tools, which could also apply to time-delayed systems, the latter being used only in such exceptional circumstances and not in any other. The contrary could lead to an unreasonable extension of the use of the technique to purposes that, due to their limited nature, do not require it.

Finally, the data may be further used for purposes other than the initial one[563], either by the same or by another controller (art. 4.2 LED). In this case, such processing is permitted provided that a) the controller is authorized to process such personal data for new purposes and b) it is necessary and proportionate for those purposes, according to Union or Member State law. Therefore, the law's maintenance purposes do not in

[561] A29 WP, *Opinion on some key issues of the Law Enforcement Directive...*", cit., p. 8. The need to limit biometrics to serious crimes is also highlighted in the ECHR Judgment *S. and Marper v. The United Kingdom*. See, in this regard, para. 24, where the Court holds that the principle of proportionality was respected in the police use of fingerprints because this is a proportionate response to the legislative purpose of dealing with serious crime.

Limiting the use of biometrics to specific types of crimes and investigations is a technical-organizational precondition for using these data in policing. ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit. p. 9.

[562] FRA, *Facial recognition technology...*, cit., p. 25.

[563] As will be discussed below, this poses an additional problem, that of function creep or extension of the use of the technique to purposes other than those for which it was originally intended.

themselves legitimize a reuse of the data[564], since the above safeguards must be observed. Thus, data collected for the investigation of a specific crime cannot be used to solve a different crime. Thus, an identification made by the FRs cannot be used in another investigation or by other data controllers unless it proves indispensable for the identification of specific suspects, victims or witnesses, and cannot be extended to persons who are not involved in criminal proceedings[565].

1.3.6.3. Data minimisation, accuracy, storage limitation, data security and accountability

Finally, recital 26 LED details that personal data must be adequate and relevant in relation to the purposes for which they are processed, thus requiring that they should not be excessive or kept longer than necessary. Such data should only be processed if the purpose for which it is intended to be used cannot reasonably be achieved by other means. To ensure that data are not kept longer than necessary, the controller should establish time limits for their deletion or periodic review. States should put in place appropriate safeguards for longer storage periods where there are public interest concerns or for scientific, statistical or historical use.

The principle of data minimization must be applied throughout the entire life cycle of the system (recital 69 AIA). According to this principle (art. 4.1.c) LED) image processing must be adequate, relevant and not excessive in relation to the legitimate purpose pursued. In FRs it is important because, for their operation, large amounts of images are needed to train and build the watchlists that require very varied data for the algorithm to be able to deliver more accurate results[566]. It is therefore very difficult to guarantee this principle since, for the mechanism to work properly, a large volume of data is required[567] which, as already indicated above, may even come from social networks or from indiscriminate collection in the spaces in which it is developed. One technique that can be used to ensure this principle is the elimination of raw data and biometric samples. Thus, once the template has been created, the information used to generate it and the other associated data are removed. In the case of stored data, these are erased once the case is completed[568].

---

[564] MOBILIO, G. "Your face is not new to me...", cit. p. 14.

[565] *Idem.*

[566] MOBILIO, G. "Your face is not new to me...", cit. p. 14.

[567] The problem with databases that gather a large amount of information is that the latter, independently, is harmless but, as a whole, leads to a violation of privacy. The essential premise of mass data processing techniques is that the discrete units of data joined together in such media can form an overall picture of an individual that allows prediction of his behaviour. MILLER, K. "Total surveillance, Big data, and predictive crime surveillance: Privacy's perfect storm", *Journal of Technology Law and Policiy*, vol. 19, nº. 1, 2014, p. 135.

[568] ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit., p. 11. The problem with this technique is that the police do not know in advance whether the raw data may be

Linked to the latter, i.e., in relation to the retention time to ensure the adequacy and relevance of the data, it should be noted that the mere retention of personal data by public authorities has a direct impact on the right to the protection of personal data[569], regardless of their subsequent use, as long as an automated biometric identification system inserted in the police databases containing the individual's information is used[570]. In this regard, we resort to two ECHR Judgements to illustrate the above. On the one hand, *S. and Marper v. The United Kingdom* and, on the other, *Gaughran v. The United Kingdom.* In the first, the applicants considered that the mere storage of their personal data for the purpose of taking them into account in future criminal investigations violated their right to data protection. On the contrary, the Court understands that this is not the case, given that the indefinite retention of personal information for criminal investigations is permitted under the country's regulations for the legitimate purpose of preventing crime. Therefore, it cannot be considered that all storage of personal data will interfere with this right, since everything will depend on the legislation of the country and the purposes for which it was made. In addition, the databases were not equipped with automated technology that would allow identification.

On the other hand, in the second, the applicant requests that his right to the protection of personal data be considered to have been violated by the police for having retained data relating to his DNA, fingerprints and photographs for driving with excess alcohol. As was the case with the parameters established in the previous prosecution, it is understood that the maintenance of such information is disproportionate when it is carried out on non-criminal persons, not so on the contrary, where even the storage can be indefinite for the achievement of the legitimate purpose of crime prevention. Therefore, another fundamental aspect in relation to the length of time information is kept in a database refers to the type of individuals. Both pronouncements distinguish, on the one hand, those who have committed a crime, whose data can be kept even permanently in the UK databases[571] (with greater time restrictions in most of the surrounding countries) as it is considered to be due to a general interest in crime prevention, since such data can be used in the future for that purpose; and, on the other hand, those who have not

useful to them in the future as the investigation develops. The elimination of data leads to problems of reliability, since in many cases other related information, such as location, is needed for judicial purposes.

The authors also talk about limiting the purpose of the template, which allows the system to store only the parameters necessary for identification; and about limited, non-bindable identification, which protects the subject from being over-identified. Similarly, biometric templates should only have a limited number of associated keys so that they can only be accessed and identified under conditions of strict necessity.

[569] DE BEER, D. et al. "Nouveaux éclairages de la notion de 'donnée personnelle' et application audacieuse du critère de proportionnalité", *Revue trimestrielle des droits de l'homme*, no. 21, 2010, pp. 145, 153.

[570] HERVERG, J. & VAN GYSEGHEM, J.M. "La protection des données à caractère personal...", cit., p. 63.

[571] Retention until the date of death of the individual data subject is understood to be permanent storage even if the data is deleted after death.

committed a crime and their information has to be deleted in a short period of time as their maintenance in the database is disproportionate[572].

It should be recalled that in the United Kingdom –as in other countries– data retention is allowed without a time limit, so that, even if the aforementioned right has been violated, the intrusion is not unlawful because in any case it complies with the provisions of the law[573]. Furthermore, the Court states that the Commission had previously stated that the retention and use of photographs taken during an arrest by police forces does not imply an interference with the right to data protection[574].

Thus, the ECHR in *Gaughran v. The United Kingdom* states that, in order to determine whether there is interference with the right to the protection of personal data, the elements relating to the specific context in which the data were taken and retained, the individuals from whom the sample is taken, the nature of the records, the way in which they are used and processed, and the results that can be obtained must be observed. In this pronouncement, the Court concludes that the photograph was obtained during an arrest and kept indefinitely in the police database, access to which was restricted to authorized personnel who did not have the capacity to identify photographs with FRs or other automated tools. However, the situation changes when the data can be shared with another police database that is equipped with this mechanism. Therefore, the Court concludes by affirming the affectation of the right to the protection of personal data by the retention of the image of the applicant's face from the moment in which FRs are used.

In relation to this last element, different time frames are established for storing data from public surveillance depending on the results obtained. On the one hand, if there was no match, the biometric templates of people passing through a public place should be automatically destroyed, indeed the system should not even identify them; in the event of a detection, the template can be stored only for the period strictly necessary to carry

[572] The UK national DNA database at the time of the *S. and Marper* case contained around five million profiles, the largest in the world. Of these, about one million belonged to people who had not committed a crime. DONADL, A. "The implementation of European Court of Human Rights Judgments against the UK: Unravelling the paradox", in Ziegler et al. (Dirs.), *The UK and European Human Rights. A strained relationship?"*, Hart Publishing, 2015, p. 151.

[573] On this aspect COGHLAN, N "*Gaughran* [2015]...", cit., p. 70, is critical. He states that the case law follows the line of observing whether the situations prosecuted are in line with the normative provisions of the State in question. The Strasbourg Court should change this criterion.

[574] See, in this regard, ECHR *Case Friedl v. Austria*, 31 January 1995, no. 15225/89. The Court raised the question whether the retention by the police of certain photographs taken in the public sphere during a demonstration could violate art. 8 of the Convention. As they had been taken without invasion of the subject's private sphere and were of public activities, the limited use made of them, the lack of intention of the authorities to identify the individuals captured in the photographs and that they were not intended for inclusion in a database, it was concluded that their retention did not constitute an infringement of the right to respect for private life.

out the police investigation[575]. After that time, the data should be automatically deleted or at least anonymized[576].

This being the case, and following the provisions of art. 4.1.e) LED, the retention of data should only be carried out for the time strictly necessary to achieve the legitimate purpose pursued, i.e., the conclusion of the investigation that motivated its processing and treatment. Any further storage and processing of data would be unlawful and would violate the right to the protection of personal data.

As for the requirement that there be no other measure less harmful to this right, we do not address it at this point because it will be dealt with in the section corresponding to the limits of rights as one of the three judgements that must be observed in the principle of proportionality.

The accuracy of biometric data can be impacted in several ways. Especially in the case of FRs in uncontrolled environments, there are external variables that can interfere with image quality, such as different angles, changes in illumination, image resolution and pixelation, changes in physical appearance due to age, illness and injury, and even similarities between individuals[577]. These are variations caused by external elements, but inaccuracies can also occur due to internal system variables[578]. To avoid these, data controllers should take all reasonable steps to ensure that the data are accurate and up to date. The adequacy of algorithms must also be ensured.

With regard to data security, any unlawful processing that may affect the accuracy and integrity of biometric data processing must be prevented and detected by preventing the destruction, loss, alteration, disclosure or unlawful transmission of personal data. To achieve this, personal data must be collected, processed and stored securely. An important preventive issue to be considered when using FRs is to avoid unauthorized access to both this technology and the data from which it is derived. This is the responsibility of the Member States. They must take the necessary measures to prevent unauthorized disclosure or access to the data, as detailed in art. 29 LED. If in the future the FRs act interconnected with other technological mechanisms, it will be very difficult to ensure

[575] Once stored for the specified period of time, it may be decided to extend it if it is found to be necessary in terms of necessity and proportionality. Retaining data for intelligence or prevention purposes is unlikely to pass a strict proportionality test because when it is collected without any specific crime, there is no reason for its storage and it would not be justified. MOBILIO, G. "Your face is not new to me...", cit. p. 15.

[576] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., pp. 524-525. To ensure such automatic data deletion, the author proposes that periodic reviews of the data be carried out.

[577] ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...," cit., p. 13.

[578] *Ibd.*, p. 14. The authors point out that, in addition, accuracy is linked to the principle of proportionality with respect to the appropriateness of an interference, minimization of prosecution and completeness of evidence.

the limitation of the use of the data[579]. For this reason, technical measures must be adopted to increase the security of the data[580].

One of them could be the pseudonymization of data (art. 20 LED on data protection by design and by default), understood according to art. 5.5 LED as the processing of personal data in such a way that they cannot be attributed to a specific individual without using additional information, provided that the latter is obtained separately and is subject to measures aimed at ensuring that the personal data are not attributable to a natural person, whether identified or identifiable. In our case, as the image of the face already makes it possible to identify a person without the need to link it to other parameters, this process would consist of altering, hiding and removing the content of the image of the face so that it would no longer be identifiable. The above immediately conflicts with the purpose of biometric identification and, specifically, with facial recognition, insofar as any database used for this purpose requires individuals to be identifiable in order for it to be used[581]. For this reason, it could not be applied and other measures would have to be sought to ensure data security.

To conclude with the study of this section, we note that European legislation leaves a wide margin of discretion to the States when deciding on the limitation of the requirements analysed here, as it does not specify any minimum standard. Thus, they can autonomously compare the interests at stake and define the situations that legitimize such limitations, which in many cases are not justified. This would result in a non-transparent use of FR technology that would not follow the lines set by existing legislation on personal data protection, which would violate this right.

For all the above reasons, it can be concluded that the protection of personal data is one of the rights most endangered by the use of FRs in public places by LEAs. This is due to the treatment of face biometrics. For this reason, specific and concrete requirements must be observed, aimed at reducing this risk as much as possible, taking into account the provisions of the AIA and data protection regulations.

1.4.Personal identity

The ability to uniquely identify individuals and associate personal attributes with them is a fundamental task in human society, as it allows individuals to identify themselves as well as to detect individual and collective similarities, identifying others as members of collectives through the recording, inference and processing of both verbal and non-verbal information, and allows the adjustment of behaviour to individual during

[579] FRA, *Facial recognition technology...*, cit., p. 25.

[580] Data security can be compromised by mismanagement and misuse of databases, which can be compromised by illegitimate access to them, resulting in data manipulation, theft or misuse. MITCHELL, A. "Distinguishing friend from foe...", cit., pp. 303-304.

[581] JASSERAND, C. "Massive Facial Database and the GDPR...", cit., pp. 185-186.

the process[582]. For this to take place, bodily characteristics such as face, voice and gait are often used in conjunction with other contextual information (i.e., location and dress). This set of attributes associated with an individual makes up his or her personal identity[583]. Biometric data are the inherent physical or behavioural characteristics of the individual that make him or her recognizable and shape his or her own identity[584]. In relation to the face, as we have already had the opportunity to explain above, it is the most consistent public aspect of our personality and our lives, through which we can visually identify others and know their feelings and thoughts[585]. For this reason, it is an essential part of our own identity through which we can easily know who a person is.

Personal identity has traditionally been considered as the right not to have one's personality misrepresented and, above all, with the interest considered worthy of legal protection, represented in the sphere of relations with one's true identity, as it is known in the social reality, general or particular[586]. Moreover, moral and social identity is understood only in terms of the environment in which individuals develop[587].

The construction of identity is closely linked to privacy, since it is shaped through the interaction of the individual with his environment and with others. Thus, if this capacity is limited because it is compromised, the right to the shaping of personal identity is violated[588]. Not only that, but also, as each individual is composed of his own information –which constitutes his idiosyncrasy–, a breach of privacy of the same is an aggression to personal identity. Thus, protecting the former is equivalent to safeguarding the latter[589].

What happens with the use of RBIS in the public sphere, as already indicated, is that it interferes with the right to privacy and this can produce chilling effects or, in other words, affect the exercise of other rights in the sense that the individual would restrict his or her actions for fear of being observed by surveillance systems equipped with FR mechanisms. Thus, police use of these mechanisms limits individual autonomy because

[582] JENKINS, R. "Identity, surveillance and modernity", Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 159-160.

[583] BEHRENSEN argues that if it can be established what makes an individual a unique person, they can also establish the conditions necessary for their continued existence as that person over time, constituting their identity. BEHRENSEN, M. "Identity as convention: Biometric Passports and the promise of security", *Journal of Information, Communication and Ethics in Society*, vol. 12, nº. 1, 2014, p. 47.

[584] Biometrics is the process of identification with which we try to find out what characteristics make individuals recognizable and not the elements that constitute you as a person. KIND, A. "Biometrics and the metaphysics of personal identity", *IET Biometrics*, vol. 12, nº. 1, 2023, p. 178.

[585] HALE, B. "Identity crisis: face recognition technology and freedom of the will", *Ethics Place and Environment*, vol. 8, nº. 2, 2005, p. 142.

[586] RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità...", cit. pp. 363-364.

[587] MARSHALL, J. *Personal Freedom through Human Rights Law...*, cit., p. 89.

[588] This relationship between privacy and the construction of one's own image has been the subject of much debate. See, for example, NERONI REZENDE, I. *Surveillance risks in IOT applied to Smart cities...*, cit., pp. 114-115.

[589] HIRANANDANI, V. "Privacy and security in the digital age...", cit., p. 1098. The author states that each individual is shaped by his information, so whatever is done to the latter, is done to him.

it usurps the capacity to act morally and, therefore, identity and its construction[590]. Along these lines, as HIRANANDANI asserts, total transparency in the name of security could result in a limited protection of physical security and a high erosion of personal and individual identity[591].

But not only that, it can also be altered from the moment biometrics is able to redefine the body in terms of information in the digital realm. This is because the digitization of certain bodily elements would affect the representation of oneself in a process of "disembodiment" that would reach our inner nature, i.e., our human essence[592]. The processing and digitization of physical and behavioural aspects is not trivial, since digital representations entail the simplification and consequent modification of the nature of the individual. The relationship between the body and identity is irrevocably changed because a machine is able to read the characteristics of the body, which are then subject to subsequent use by biometric instruments, without time limit and wherever the person is[593]. Consequently, biometrics turns people into objects that can be measured and compared with other similar objects[594]. Likewise, there is a process of dehumanization that affects personal identity, since it causes the redefinition of some elements of the body and their conversion into digital parameters suitable for identification, which also affects, as already mentioned, dignity.

For this reason, we are dealing with a right deserving of protection in itself, which is placed at the disposal of the right to a name and image. On the one hand, personal identity serves to identify others, that is, to make it clear that an individual is specifically the person he or she claims to be; and, on the other hand, it can be pointed out as the characterizing element of the person, an integral part of it and instrumental for its full development, altered by the biometric processing of personal data and its identifying potential. Therefore, in view of its importance, it requires specific protection. In short, identity represents the image of the person, which is composed of two elements: the consideration that the individual himself and others have about him and the visual aspect

[590] HALE, B. "Identity crisis...", cit., p. 142. The author continues his argument by pointing out that the threat of external repercussions has detrimental effects on the ability of citizens to make decisions based on moral grounds, being, in his opinion, the reason for opposing the use of this technology, rather than for reasons of privacy or objective freedom.

On the contrary, other authors consider that the ethical implications related to the use of biometrics in identity management are not linked to identity but to privacy and dignity. In this sense, BEHRENSEN, M. "Identity as convention...", cit., p. 52. However, he understands that both would be the essential piece of oneself, so he links them again with personal identity.

[591] HIRANANDANI, V. "Privacy and security in the digital age...", cit. p. 1098.

[592] MORDINI, E. & MASSARI, S. "Body, biometrics and identity", *Bioethics*, vol. 22, nº. 9, 2008, p. 494.

[593] See, Opinion of Advocate General Mengozzi of 13 June 2013, Case C-291/12. Michael Schwarz v. Stadt Bochum, p. 1.

[594] MORDINI, E. & MASSARI, S. "Body, biometrics and identity...", cit. p. 494.

that allows his unequivocal identification[595] in the eyes of others, including, within these, the FRs.

HALE distinguishes three types of identity: institutional, photographic and practical. The first refers to facts relating to a person's public identity contained mostly in archives. The second is the one most closely linked to our object of study and is embodied in the physical facts of identity, for example, a facial imprint of how one sees oneself at a given moment and the specific way in which FRs are able to identify the individual in question. Distinguishing the first two, photographic identity involves the identification of a person and institutional identity is his or her composite identity[596], i.e., the set of elements that make up all that he or she is outwardly. Finally, practical identity is the conceptual and normative assumptions that accompany one's own conception of oneself[597]. In this sense, uniting all these perspectives, it can be stated that identity is the result not only of an identifying activity, but also of a process of (re)construction of the individual personality, corresponding to the set of elements that characterize a person and make him or her unique and singular.

Therefore, identity can only be represented as a *quid pluris* with respect to identification, claiming an *ad hoc* protection, having previously carried out a necessarily extensive interpretation of the signs of identification. Thus, a relationship of instrumentality and reciprocity is revealed between identity and identification[598], since one depends on the other. In this sense, it must be taken into account that identification and identity are two concepts united but distant at the same time[599]. This statement is due to the fact that the former is the process by which the identity of a subject is established, while the latter would be composed of all the elements that make up his or her idiosyncrasy both at the individual and social levels.

It is on the basis of this personal identity projected to the community (through photographic identity or image) that FRs will be able to detect a person in an uncontrolled environment on the basis of the information contained in a watchlist. The identification tools go beyond the identity itself, being naturally circumscribed to a physical and material domain, linked to the exteriority[600]. Whether it is the face information that makes it possible to identify an individual or his telephone number or address, all these elements constitute information that does not require recourse to the digital sphere for identification. When the leap to the digital sphere is made, the issue becomes more

[595] RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità...", cit. p. 364.

[596] HALE, B. "Identity crisis...", cit. p. 143.

[597] *Idem.*

[598] RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità...", cit., p. 365.

[599] *Ibd.*, 365. The same authors on p. 368 conclude that the success of the digital transition implies an alteration of the relationship between the traditional categories of identification and personal identity, whose boundaries are inevitably becoming blurred, making it more difficult to distinguish where one begins and the other ends.

[600] *Idem*.

complicated and the essential content of this right may be damaged or, at least, restricted, since if individuals limit their social activity because they believe they are subject to a state of surveillance, the shaping and exercise of their identity is compromised.

With the development and extension of FRs, the line between the private and public spheres has become blurred, since the face information, when in a space equipped with this technique, becomes available for the same, which is capable of capturing and processing it. This situation, taken to the extreme, could facilitate to those who have control over such systems, a disproportionate and irrational use that can lead to a state of mass surveillance in which espionage and control of citizens would be a constant. It is true that it could be effective in the fight against crime, since individuals who are being sought by the police for having committed a serious crime or terrorist attack or there is a known threat that they may do so, would be detected quickly, which would facilitate their arrest and, thus, the maintenance of public order seriously threatened by crime would be achieved.

However, it may also happen that a citizen decides not to participate in social activities such as, for example, meetings in public environments or demonstrations (as will be discussed below) for fear of being identified and tracked by the mechanisms and that this information can be linked to another[601] forming his profile that can be known and used for various purposes, whether political, economic or otherwise. Therefore, the right to personal identity is strongly threatened, if not restricted, by FRs, limiting the capacity for personal self-determination in favour of these insidious systems.

1.5.Self-image

This right to one's own image is closely linked to personal identity and its development[602] as well as to the privacy and dignity of the person[603]. This is clear from the Judgement of the ECHR *Case Von Hannover v. Germany*, which states that the image is one of the main attributes of the personality of an individual because it expresses his originality and allows him to differentiate himself from others. Thus, the right to image protection is one of the essential prerequisites for personal development and, therefore,

[601] HALE, B. "Identity crisis...", cit. p. 150.

[602] Judgment ECHR *Case Papageorgiou and others v. Greece*, 31 October 2019, nº. 4762/18 and 6140/18. In the development of personal identity, the perception of self-image and the role of the individual in relation to others are important in adolescence and determine adulthood.

[603] On the relationship with the latter, see ECHR *Case Peta Deutschland v. Germany*, 8 November 2012, nº. 43481/09 when it states that, if the image of Jews is so instrumentalized, little remains of their human dignity. For its part, in the Spanish STC 81/2001, of March 26, it is held that the right to an image has as a reference the dignity of the person, which creates a necessary sphere to maintain a minimum quality of life, linked to the very existence of the individual, by saving his personal sphere by reserving it from illegitimate intrusions of third parties. In addition, it is aimed at protecting the moral dimension of persons. Thus, others are prevented from obtaining, reproducing or publishing the image of an individual by another unauthorized person, whatever the purpose.

for privacy[604]. Thus, it presupposes control over one's own image, which also includes the possibility of refusing to disclose it[605], also over the recording and subsequent storage, as evidenced in the *Case Reklos and Davourlis v. Greece* of the ECHR[606].

In the latter, the Court goes on to point out that, since the personal image is one of the characteristics linked to personality, its effective protection presupposes obtaining the consent of the person concerned. Otherwise, an essential attribute of personality would be left in the hands of third parties and the person concerned would have no control over the subsequent use of his image. In this particular case, what the Court found to be an infringement of the right to one's own image was the storage of a child's image by a doctor without parental consent, since this image allowed the doctor to use it in the future against the will of the person concerned. If we extend this situation to the use of the image of the face for inclusion in a database, either for the training of the algorithm or for subsequent processing that makes it susceptible to identification through the FRs, the individual's right to his or her own image would be infringed.

Although the latter is worthy of autonomous protection, as can be seen from the above, it is closely linked to the other aforementioned rights. However, what is special about it and what makes it independent and in need of specific assistance, is the protection against reproductions by third parties of one's own image as one's own reserved space, although not intimate from the action and knowledge of others. It is also a necessary area to be able to freely decide the development of one's own personality and maintain a minimum quality of life. This is achieved through the recognition of the power to prevent the unconditional dissemination of physical appearance as the first element shaping the personal sphere of every subject, as a basic instrument of identification and external projection, and an essential factor for recognition as an individual[607]. In short, the aim of this right is to safeguard the ability to decide which aspects of one's image one wishes to keep away from public dissemination and to keep hidden, with the aim of guaranteeing a private sphere for the development of one's own personality, free from interference by third parties.

Technological development has changed the way we understand personal image and, in our specific case, the face. Digital faces, i.e., those shared through social networks and the technologies used to capture, store and process them, alter the conditions of personal visibility, public intimacy and relationships in general. Faces acquire a new

[604] Of this opinion, FRA, *Facial recognition technology...*, cit., p. 23.

[605] Judgement ECHR *Case Von Hannover v. Germany (nº. 2)*, 7 February 2012, nº. 40660/08 and 60641/08. The Media Lawyers Association, as respondent, takes the opposite position, arguing that Art. 8 of the Convention does not create a right of image or reputation. Thus, the publication of a personal photograph by itself does not constitute an interference with the right to privacy, depending also on the context in which the photograph was taken.

[606] ECHR Judgment *Case Reklos and Davourlis v. Greece*, 15 April 2009, nº. 1234/05.

[607] Spanish STC 81/2001, of March 26, 2001.

meaning or function because in the digital environment they represent, identify, reveal, suggest, unblock, act, communicate, etc.[608].

More specifically, FRs have made difficult our understanding of communication channels, which have been mainly conceptualized in terms of human processes. The face is one of the main means of communication between people but now this process is also done with machines. When these two entities interact, humans share their fingerprints as well as metadata. To illustrate this process, BUCHER suggests the neologism "fAIce communication" as a way of conceptualizing the communication characteristic of individuals and their interactions with FR technologies and the inherent power relations at play in them[609]. Such mechanisms work in a process of abstraction and constant comparison. Faces are not only encoded but also carefully prepared to be read and identified along with the wealth of information they contain.

In the case of the use of this parameter by the LEAs, it may happen that the individual is unaware that his face is being processed for such purposes, and it may be in his mind that this attribute of his personality is private and therefore remains hidden from the view of third parties and he refuses to be processed by others. In addition to this, in the environment we are analysing, the subject could eventually be involved in situations in which he is detected by the mechanism even erroneously, thus compromising the right to his own image.

As established in the aforementioned ECHR *Case of Glukhin v. Russia*, privacy can be harmed by the systematic or permanent recording of personal data, especially images of an identified individual. The personal image is one of the characteristic attributes of the personality because it reveals the unique elements of the individual and distinguishes him from others. Thus, the right to protection of personal image is one of the essential components of development and presupposes the power to control the use of this image. Sometimes the latter includes the possibility of a subject to refuse to publish it and also to oppose its recording, conservation and reproduction by others; all of which happens with the use of FRs by agents in charge of maintaining security.

1.6.Freedom of movement

The identifications carried out through FRs are likely to limit –and greatly– the freedom of movement of individuals, understood as a component of individual freedom in a broad sense, since moving, parking and staying in one place are an integral part of the vital functions of the individual[610]. The use of this technique by law enforcement

[608] BUCHER, T. "Facing AI: conceptualizing 'fAIce communication' as the modus operandi of facial recognition systems....", cit. p. 644.

[609] *Ibd.*, pp. 647-648.

[610] PHILIPPE, X. "La liberté d'aller et de venir", in Cabrillac, R. et al. (Dirs.), *Libertés et droits fondamentaux*, Dalloz, Paris, 2007, p. 319.

agencies, especially the delayed technique, allows them to know who is linked to those involved in a given incident, to identify and locate perpetrators and witnesses of past crimes and to confirm alibis, as well as to know where a person was at a given time. In the event that an individual is identified as having committed a crime, it can even lead to the imposition of a custodial measure[611].

These practices, although they may have laudable purposes such as some of those indicated, go far beyond mere identification, as they make it easier for the location of a subject at a specific time to be known in the future[612] and can lead to the monitoring of their movements. Some U.S. case law considers that in the public sphere there is a lower expectation of privacy that also extends to personal movements, which is why the police can track the locations of a person over time[613]; while others, while reaching similar conclusions, are more nuanced, in the sense that although a public action is not completely private, it is reasonably expected that the sum total of all movements is[614] and, therefore, is not subject to monitoring. In this sense, FRETTY talks about "location privacy" and the challenge that monitoring through FRs[615] poses to it in the long term. Something similar occurs with real-time geolocation through GPS devices. In relation to them, the ECHR in the *Case Ben Faiza v. France*, admits that, when used in real time, it is an investigative technique that allows live tracking of the movements of a person or object, constituting both this type of surveillance and the processing and use of the data derived from it, an interference in the private life of those to whom the measure is directed[616].

The fact that an individual can be identified wherever he goes, regardless of the exhaustive tracking of the places he visits, has a strong intimidating effect since not only this information can be known but also, in a process of data aggregation, his political and religious ties and the people he frequents. This issue particularly jeopardizes the free

[611] On the restriction of the right to ambulatory freedom by the use of AIs, see AMONI REVERÓN, G.A. "Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal", in Cotino Hueso, L. (Dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, pp. 193-236.

[612] FRETTY, D.A. "Face-recognition surveillance: A moment of truth for fourth amendment rights in public places," *Virginia Journal of Law & Technology*, vol. 16, nº. 2, 2011, p. 450.

[613] In this regard, see, for example, *Ibd.*

[614] *Ibd.*, p. 451. In that sense, although a motorist may be monitored 24 hours a day by GPS, he reasonably expects not to be monitored without an arrest warrant. Similarly, LOVALLO, C. "Big Brother's fall brings liberty to all: Addressing the urgency for strict regulation governing law enforcement use of facial recognition technology in Texas", *Thurgood Marshall Law Review*, vol. 46, nº. 1, 2021, p. 84.

Thus, having a GPS device installed in a vehicle and recording its movements for an extended period of time constitutes an investigation under the Fourth Amendment. It further establishes the right of individuals to be secure in their homes, papers and effects against unreasonable searches, and requires that search warrants be adopted for each case. The author goes on to note that while a GPS is not a FR tool, its use is very similar in the law enforcement setting.

[615] FRETTY, D.A. "Face-recognition surveillance...", cit., p. 451.

[616] ECHR *Case Ben Faiza v. France*, 8 May 2018, no. 31446/12, para. 53. In para. 54 it argues that when geolocation is coupled with other measures such as the interception of telephone communications, a subject is subjected to a particularly close surveillance device, involving a superior interference.

exercise of the rights of assembly, association and demonstration, thus shaking the foundations on which democracy is based.

In this line, we bring up the example of the dystopian society presented by George Orwell in *1984*, in which all citizen movements were under constant surveillance and the State knew every individual step of all members of the population because, among other surveillance techniques, there were cameras installed in both public and private spaces and sensors capable of capturing all sound, so that there was no privacy even in one's own home. This situation generated uncertainty and fear because it was impossible to know if at any given moment one was being recorded, which is why society saw the exercise of their rights very restricted, especially their freedom of movement, as they were not allowed to frequent certain areas of the city or other people.

Illustrative of the situation we have just indicated is the following passage from the work, which we reproduce: "The telescreen received and transmitted at the same time. It was able to pick up any sound Winston [the protagonist of the novel] made above a very low whisper; what's more, as long as he was in the field of vision dominated by the metal plate they could see and hear him. Of course, it was impossible to know whether they were watching you or not at any given moment. How often or with what system the Thought Police turned on one's screen was pure conjecture. It was even conceivable that they were watching everyone at the same time. In any case, they could connect with you whenever they wanted. You had to live –and habit eventually became instinct– assuming that they listened to every sound you made and, except in the dark, watched your every move. Winston continued with his back to the telescreen. It was safer; although he knew very well that even a back could be revealing. (...) Sitting in that alcove as close to the wall as possible, Winston was out of the telescreen's field of vision. Of course, they could still hear him, but as long as he was still there they could not see him"[617].

The above is illustrative of a scenario of mass state surveillance promoted by the power conferred by the indiscriminate use of new technologies, including FRs. In reality, this does not happen in such an extreme form today, but in some totalitarian regimes, such as China's, they are already being used to control certain segments of the population. Thus, China has implemented face recognition mechanisms in the Xinjiang region to monitor millions of Uyghur and ethnic minority citizens. The government justifies this application as a means to act against Islamic radicalization and prevent terrorism. However, it is actually carrying out surveillance work and has even set up "re-education" camps to control these people. The inhabitants of this region are under a state of constant surveillance through this biometric system that uses large databases in which information on facial parameters is combined with other information such as name, address, date of birth, identity document, place of work, etc. In addition, a list of frequented places is

[617] ORWELL, G. *1984*, Penguin Random House Editorial Group, 24th reprint, 2023, pp. 10-13.

added and accumulates in real time the movements of all the individuals included in the same[618].

Not only that, but in other cities the FR technique is also being used to control minor infractions such as the practice of "jaywalking", which can be defined as "a pedestrian's choice to disobey specific road rules and cross the road without regard for oncoming traffic"[619]. The term would include the action of crossing the road when the traffic light is red or in a place where there is no crosswalk. It is true that this activity has a negative impact on the flow of vehicles, including increased delays, excessive fuel consumption and increased emissions[620], but we consider it excessive that in China FRs have been implemented to detect these alleged "violators" and stop them. The mechanisms are linked to a government database that contains information on the population and through it, residents who jaywalk are identified. That is not the end of the matter, since once detected, the name and face of the individual is projected on a large electronic screen next to the place where it happens[621]. If this is already embarrassing, it is even more so when the system fails to detect. It happened to Dong Mingzhu, a well-known businesswoman in the country, who was accused in the city of Ningbo of having crossed a crosswalk wrongly when in fact she was not actually at that moment in the place where the detection occurred, but the system identified a promotional image of her on a bus[622]. Thus, the system mistook an advertisement for a real person and issued the alleged camera violation when it had not been committed. In addition, in other cities such as Beijing, the police use various devices equipped with FRs such as smart glasses to identify in real time any person on a watchlist[623].

---

[618] For more on the issue, see VIDAL LIY, M. "2.5 millones de personas en China, bajo el control de una empresa de vigilancia facial...", cit.; & COLLINS, J. "China is using facial recognition to track millions of Muslim citizens wherever they go...", cit.

The Asian country does not only make use of facial recognition for these purposes, since during the hardest period of the coronavirus pandemic, it used it as a tool to fight against it. To this end, it implemented it in public places such as underground subway stations in different cities to scan crowds in search of people with fever or to identify those who were not wearing masks. JAKHAR, P. "Coronavirus: the innovative technologies China is using to combat COVID-19 (and the concerns they raise), *BBC*, March 4, 2020. Electronic resource obtained via the Web: https://www.bbc.com/mundo/noticias-51736635, [retrieved on 28 July 2024].

[619] SHIWAKOTI, N. et al. "Exploring Jaywalking and Intersections", *39th Australasian transport research forum*, Auckland, New Zealand, 2017, p. 1. On p. 5 the authors state that there are different types of violations: 1) starting to cross when the red signal is flashing; 2) crossing with the red signal; and 3) jaywalking. This last action refers to the scenario in which a pedestrian who crosses the street incorrectly first influences others to follow. Some elements that may have an impact are: 1) social interaction; 2) using a cell phone; 3) talking on the phone; and 4) using headphones.

[620] ANIK, M.A.H. et al. "Investigation of pedestrian jaywalking behavior at mid-block locations using artificial neural networks," *Safety Science*, vol. 144, 2021, p. 1.

[621] DAUVERGNE, P. *Identified, tracked, and profiled: The politics of resisting facial recognition technology*, Edward Elgar Publishing, 2022, p. 2.

[622] BBC, *Chinese AI caught out by face in bus ad*, 27 November 2018. Electronic resource obtained from World Wide Web: https://www.bbc.com/news/technology-46357004, [retrieved 28 July 2024].

[623] DAUVERGNE, P. *Identified, tracked, and profiled...*, cit., pp. 2-3. In other areas, the technique is also being implemented for various purposes, such as at school to control attendance and monitor hallways. A school in the city of Hangzhou has gone even further by starting to use emotion recognition

Thus, freedom of movement is seriously compromised by the use of FRs from the moment in which they allow unprecedented control of citizens and monitor the steps of all members of the population, even being able, in a process of aggregation, to join this information with other personal information that can cause individuals a feeling of constant surveillance and, as a result, restrict their movements and participation in activities such as demonstrations, which also violates the right to freedom of assembly, demonstration and strike, which we will analyse more extensively in the following section.

2. Individual freedoms in their social dimension: expression, association, reunion, demonstration and strike

The right to freedom of expression, included in art. 10 of the Convention[624] and 11 of the Charter, has as one of its manifestations that of peaceful assembly –which includes demonstrations, strikes, rallies, etc.[625]– and of association, included in art. 11 of the first[626] and 12 of the second. Meetings play a very important role in democratic society because they constitute a means for the exercise of other rights, since they facilitate the mobilization of the population in the celebration of events through which claims and aspirations are formulated, thus influencing state public policy[627]. On the other hand, it should be noted that this right does not cover all types of meetings, but only those of a

technology to scan facial expressions during classes and detect signals such as boredom, sadness, anger and scepticism.

[624] This article specifically states the following: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

[625] On the concept of "assembly" and all the activities it includes, see, HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai*, 2012, para. 24.

[626] "Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and join trade unions for the protection of his interests. 2. No restrictions shall be placed on the exercise of these rights other such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State".

[627] HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, cit., para. 24.

This right is especially important for those who are not part of a political party, as it gives an individual the opportunity to communicate opinions and share them with others, attract media attention and participate in public debates. SIEGERT, K. "The police and the human right to peaceful assembly", in Alleweldt & Fickenscher (Eds.), *The police and international human rights law*, Springer, 2018, p. 218.

non-violent nature and in which the participants have peaceful intentions, it being a different matter if during such meetings a violent incident occurs.

New technologies have a positive impact on the exercise of this right because, among other aspects, they allow the mobilization and organization of protests, and improve transparency and accountability for any abuses that may occur during their development[628]. However, they also have some negative aspects, linked to the risks in the exercise of rights posed by surveillance through such systems. This is because they have considerably expanded the capacity of state authorities to monitor protests, especially through the FRs[629].

The Special Rapporteur of the United Nations Human Rights Council in 2019 expressed his concern about the proportionality of the implementation of these systems in peaceful assemblies, insofar as we are dealing with a technique of identification and data collection that undermines the anonymity of the individual in public spaces and has deterrent effects on the decision to participate in such events[630]. Therefore, it argues that the use of surveillance technologies to indiscriminately and generally control those exercising their rights to peaceful assembly and association should be prohibited. Despite this, it adds as an exception the existence of reasonable suspicion that certain individuals are involved in serious crimes or are planning to become involved in them, taking into account strict standards and the principles of necessity and proportionality, under strict judicial supervision[631].

The United Nations High Commissioner for Human Rights notes that FRs have very detrimental effects on this right alongside those of privacy, personal identity and freedom of expression. In this sense, it states that deploying this technique in meetings and demonstrations causes a huge and indiscriminate interference in the latter two because it requires collecting and processing facial images of all persons captured by surveillance systems that have it incorporated or connected to it[632]. Already the introduction of visual recording systems weakened the protection of individuals participating in meetings and demonstrations. Today, such protection is further reduced with the introduction of facial recognition mechanisms as it drastically increases the ability to automatically identify participants in such events, raising major problems because it favours surveillance and selective tracking. If done in real time, it even makes it possible for security forces to intervene to break up a peaceful meeting or demonstration. Therefore, it has serious detrimental effects on this right where it can reach

[628] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies*, cit., para. 7.

[629] *Ibd.*, para. 24.

[630] HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and association*, 2019, para. 56.

[631] *Ibd.*, para. 57.

[632] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies*, cit., para. 33.

large dimensions and cause many people to feel dissuaded from exercising it for fear of being identified and suffering negative consequences[633].

Thus, as can be seen, the importance of this right in our object of study is undeniable, not only because of everything mentioned so far, but also because of the fact that the only two existing judicial pronouncements to date on FRs in public spaces for police purposes have been motivated by their use in peaceful demonstrations.

As we have had occasion to explain in the previous section, the spread of biometric identification –which may become massive– will inevitably alter human behaviour, in the sense of restricting the movements of individuals. This has enormous implications for our democratic values. Along these lines, any public expression of dissent or criticism towards the state apparatus could be identified by the FRs and taken as a threat to the government, and could be quickly dealt with; furthermore, they would be used to label and coerce those who publicly express their opinions, labelling them as criminals even when they participate in peaceful meetings or demonstrations[634]. This situation would lead to a change in the places visited, the people with whom one associates or meets, and one could even stop attending social or religious events for fear of being identified by the systems when participating in such events[635], including demonstrations and protests. In this sense, the feelings of intimidation that people may suffer if they reasonably believe that their behaviour may be monitored and controlled has the effect of restricting the right to freedom of expression that is materialized through attendance at such events. So that, in an exercise of weighing interests, they would decide to keep their image private and thus not put their personal data at risk, thereby diminishing the ability to express ideas and opinions, communicate with others and participate in democratic processes.

Intensive police surveillance during the development of a demonstration can reveal all kinds of personal information, including sensitive data such as political affiliation or religious beliefs[636], from which chilling effects are derived. In this sense, recital 32 of the AIA states that this feeling of constant surveillance can indirectly dissuade citizens from exercising this right. Thus, individuals, fearing that their personal

[633] *Ibd*, para. 34; & EUROPEAN COMMISSIOIN FOR DEMOCRACY THROUGHT LAW (Venice Commission) & OSCE OFFICE FOR DEMOCRATIC INSTITUTIONS AND HUMAN RIGHTS (OSCE/ODIHR), *Guidelines of Peaceful Assembly (3rd Edition)*, 2019, para. 172.

[634] SANABRIA MOYANO, J.E. et al. "Tecnología de reconocimiento facial y sus riesgos en los derechos humanos", *Revista Criminalidad*, vol. 64, nº. 3, 2022, p. 71.

[635] As ASHRAF states, for example, using Clearview AI, LEAs or state intelligence agencies can identify individuals through cross-referenced social media profiles and posts by providing a random photograph of someone going to a church, mosque, synagogue or any other place with religious connotations. ASHRAF, C. "Exploring the impacts of artificial intelligence on freedom of religion or belief online," *The International Journal of Human Rights*, vol. 26, nº. 5, 2022, p. 776.

[636] Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance. Freedom to manifest one's religion or beliefs shall be subject only in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others".

information may be collected and used by the police, may decide not to attend such events[637] and stop exercising their legitimate rights.

This situation is illustrated in the ECHR *Case Catt v. The United Kingdom*. It arises from the inclusion in the police "Extremism Database" of some personal information of the applicant, specifically relating to his participation in lawful and, in principle, peaceful demonstrations. It is true that in some of these demonstrations there was disorder and criminal acts and the interested party was stopped by the police twice for obstruction of the public highway, but he was never convicted of any crime. The database contained not only this information but also other personal information such as name, date of birth, address and, in some cases, a description of his appearance and photographs. Therefore, the applicant claims a violation of his right to privacy inasmuch as the storage of data was excessive and unnecessary. Furthermore, the retention was unjustified because the data related to his participation in lawful political protests and the information was not useful for the execution of police functions and was likely to cause chilling effects. The Court decided in their favour, emphasizing the risk of such effects as well as the fact that the database did not contain minimum safeguards. As interesting as the pronouncement is, the conclusion of the opinion of Judge Koskelo joined by Judge Felici is even more interesting. The former proclaims that the person concerned, who has never been charged with any crime or accused of violence, nor has he ever been suspected of involvement in criminal activities, ends up having his personal data on his participation in demonstrations and union events recorded in a database. For this reason, his peaceful exercise of the rights enshrined in articles 10 and 11 of the Convention is impaired.

As can be seen from the above, the collection and storage of the personal data indicated, even without using the FRs or any other technique based on biometrics, involves interference in the rights to freedom of expression and freedom of assembly and association, as enshrined in arts. 10 and 11 of the Convention, respectively. Thus, the interference will be even greater in the case of using such mechanisms because they allow knowing immediately –in those that act in real time– or in a longer period of time, that a person is (or has been) participating in a certain public event and that information can be used as a reason for police persecution or to keep it under control in order to prevent crime, as in the case described above; or to justify an arrest as happened in the case of *Glukhin v. Russia,* which, remember, involves a person's participation in a certain public event, more specific citizen who had carried out a peaceful protest alone. He was identified, arrested and prosecuted sometime later using a combination of FRs and retrospective analysis of the recordings. The Court concluded that the highly intrusive use of FRs was a disproportionate response to the protest, especially since it posed no security risk.

[637] AKHTAR, M. "Police use of facial recognition technology and the right to privacy and data protection in Europe", *Nordic Journal of Law and Social Research*, no. 9, 2019, p. 339. Similarly, LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit., p. 7. The author argues that the detrimental effects are higher in totalitarian regimes.

In this terms, it should be noted that, even when the images have not been taken directly by a FRs, this technology can be used once the recordings have been captured by conventional surveillance mechanisms to which an automated biometric identification mechanism can subsequently be applied[638]. In our opinion, this situation is even more detrimental to the rights and freedoms of citizens than the use of mechanisms that act in real time (where it is assumed that LEAs have the duty to inform that the area is being monitored by such systems, except under certain circumstances). This is because the police, surreptitiously, could make use of this technology once some time has elapsed since the event took place, this point being totally unknown to the participants in the event.

The other judicial resolution on FRs is *R Bridges v. CCSWP and SSHD*. In this case, the use of these systems was prosecuted at two specific times. In one of them, the applicannt was participating in a demonstration very close to the place that was being monitored by such mechanisms. The argument put forward by the interested party was the non-existence of a legal basis for the use of this technology and the unjustified impact on the right to freedom of expression. The Court of Appeal found that the South Wales Police resorted to this tool with a wide margin of discretion in the place and manner of execution, and was capable of infringing on the right to freedom of expression and limiting people from exercising their right to protest. Notwithstanding the above, it concluded that its deployment was proportionate to achieve the intended objectives of crime prevention, in view of the results obtained.

3. Prohibition of discrimination

The FRs, since they allow the processing of large amounts of data, carry the risk of false results and discrimination[639]. The latter occurs when a person or group is treated less favourably than another in an identical situation[640]. The prohibition of this practice on grounds of sex, race, colour, ethnic or social origin, genetic characteristics, language, religion or belief, political or any other opinion, membership of a minority, property, birth, disability, age or sexual orientation, is set forth in Art. 21 of the Charter, the content of which corresponds to the provisions of in art. 14 of the Convention (which also establishes the duty to guarantee the enjoyment of rights and freedoms without distinction of any kind on the above grounds), but the former is broader, since the list of rights is not exhaustive and is open to the protection of new ones.

In the *White Paper on Artificial Intelligence*, the European Commission establishes discrimination as one of the major problems faced by AIs; and, in para. 44 of

[638] COUCHMAN, H. "Mass Surveillance on Our Streets...", cit., pp. 586-587.

[639] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 2.0...*, cit., p. 5.

[640] FRA, *Facial recognition technology...*, cit., p. 27.

the *Ethics Guidelines for Trustworthy Artificial Intelligence*, the High-Level Expert Group on AI also refers to the right to non-discrimination, which implies that the operation of AIs should not generate unfairly biased results, which requires respect for potentially vulnerable individuals and groups. Likewise, it establishes as one of the essential principles of these mechanisms, equity, which, among other issues, aims to ensure that no unfair bias, discrimination or stigmatization is suffered. It goes on to point out that, if the former are avoided, AIs could increase social equity. For its part, in the *Recommendation on the Ethics of Artificial Intelligence*, UNESCO highlights equity and non-discrimination as one of the principles for reliable AI. To safeguard it, actors must make every effort to minimize and avoid reinforcing or perpetuating discriminatory or biased applications and outcomes throughout the life cycle of systems to ensure their fairness. Thus, an effective remedy against discrimination and biased algorithmic determination should be available.

AIs are not infallible and have inherent biases of their creators because they unconsciously insert their own biases when selecting the data and coding the algorithms to develop the mechanism[641]. For that reason, their results are not completely reliable and serious bias and discrimination can result from the interpretation of the results[642]. Likewise, there is no biometric system at present that provides completely reliable and absolute results[643]. Therefore, like the others, FRs produce results in probabilistic terms, i.e., they are scores that show a certain percentage of probability of the existence or not of a certain fact, or of making or not making a decision[644]. In this case, we are dealing with a probabilistic technology that makes it possible to automatically recognize the identity of individuals based on the characteristics of their face[645]. The comparison

[641] MUNARINI, M. "New perspectives on the mitigation of gender bias in AI by EU regulations...", cit., p. 112. Similarly, ZUIDERVEEN BORGESIUS, F.J. "Strengthening legal protection against discrimination by algorithms and artificial intelligence", *The International Journal of Human Rights*, vol. 24, nº. 10, 2020, p. 1575, when he admits that if a system is trained with biased data, it runs the risk of reproducing such biases.

[642] As can be seen from recital 28 AIA, these mechanisms can be misused and enable practices of manipulation, exploitation and social control. Such practices are highly damaging and improper and must be prohibited, as they run counter to the Union's values of respect for human dignity, freedom, equality, democracy and the rule of law, as well as the fundamental rights of the Charter, including non-discrimination.

Similarly, the High-Level Expert Group on AI, in para. 80 of the *Ethics Guidelines for Trustworthy Artificial Intelligence*, expressed the need to avoid unfair biases. To this end, the datasets used by AIs should be observed as they may have inadvertent historical biases whose maintenance could lead to (in)direct and unintentional prejudice and discrimination against groups or individuals, which could exacerbate stereotyping and marginalization. It may even be the case that biases are intentionally exploited. Wherever possible, identifiable and discriminatory biases should be eliminated already at the information gathering stage.

Also the *Recommendation on the Ethics of Artificial Intelligence*, adopted on November 23, 2021 by UNESCO, emphasizes that one of the major concerns of AI is the biases that it can embody or exacerbate and thus lead to discrimination.

[643] De HERT, P. "Biometrics: legal issues and implications", *Background Paper for the Institute of Prospective Technological Studies, DG JRC-Sevilla, European Commission*, 2005, p. 7.

[644] NOVOKMET, A. et al. "Facial recognition technology in EU criminal justice...", cit., p. 550.

[645] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 9.

between the real image and the one contained in a database deduces a greater or lesser probability of correspondence between the two. If this probability exceeds a certain threshold, defined by the user or developer of the system, a match is made[646]. There is therefore a margin of error, so the identification will not be completely accurate and correct[647] and, although the failure rate can be reduced with technological advances, the verdict can never be absolute.

Although there are appropriate circumstances, such as its use in controlled spaces with good luminosity and sophisticated image acquisition systems, this technology raises questions of inaccuracy[648]. Among other things, because, as the FRA states, we must bear in mind that "an algorithm never returns a definitive result, but only probabilities"[649]. In its report on the impact of new technologies on the right to peaceful assembly and demonstration, the United Nations High Commissioner for Human Rights maintains that FRs entail significant risks for its enjoyment, for all the reasons mentioned above, since we are not dealing with an infallible technology and it is still prone to errors. Even when used with a large number of people, its lowest error rate can mean inaccurate signalling of hundreds of them[650]. For this reason, it is capable of perpetuating and amplifying discrimination against certain population groups, as it can also be used to profile individuals based on ethnicity, race, origin, gender, etc. It can also lead to unintentional discrimination[651] because its accuracy depends on factors such as skin colour or gender[652].

Racial discrimination is one of the most common when FRs are used and occurs when a person is subjected to police check because of a decision based exclusively or

[646] *Ibd.*, p. 10.

[647] ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...," cit., p. 6.

[648] RAPOSO, V.L. "Health, privacy and liberty...", cit., p. 534.

[649] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*..., cit., p. 9. The UN Human Rights Council also alludes to the likelihood of the outcome of biometric systems. HUMAN RIGHTS COUNCIL, *The Right to Privacy in the Digital Age*..., cit., p. 8.

See, furthermore, COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit, p. 127. The author points out that the FR-based technique performs the search for a match based on a percentage index; NERONI REZENDE, I. *Surveillance risks in IOT applied to Smart cities*..., cit., p. 204; & MOBILIO, G. "Profilare tramite riconoscimento faciale...", cit., p. 186.

[650] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0*..., cit., p. 13.

[651] In general, the term *profiling* refers to the practice of law enforcement using certain personal characteristics as indicators of suspicious behaviour. In the case of racial profiling, it would be the development of police operations towards specific subjects based on physical, racial or ethnicity-related characteristics. Thus, the practice is based on the assumption that people with certain characteristics are more likely to commit certain crimes. PELAIA, C. & NUCERA, G.G. "La prassi del *racial profiling* in Europa: Una forma di discriminazione istituzionale", *I Diritti dell'Uomo*, vol. 27, nº. 1, 2016, p. 82.

In relation to the profiling that can be carried out through FRs, BUCHER already points out that it is the very essence of these mechanisms, when he states that their development is based on a type of biological essentialism that works to arbitrarily divide human populations based on facial characteristics. It thus serves to classify people, especially in terms of imposing a category of race. It allows a coding process that goes beyond a neutral or egalitarian procedure given that many faces communicate better than others in the face of the machine. This results in many misidentifications that can produce discriminatory effects. BUCHER, T. "Facing AI: conceptualizing 'fAIce communication' as the modus operandi of facial recognition systems...", cit. p. 645.

[652] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies*, cit., para. 32.

primarily on their race, ethnic origin or religion when, had it not been for these characteristics, the inspection would not have taken place[653].

The AIA, specifically in recital 32, highlights the concern about the technical inaccuracies of the FRs that can lead to biased results and have discriminatory effects. It goes on to note that this is especially significant in the case of systems that act in real time because the immediacy of the consequences and the limited opportunities for checks or corrections increase the risk. However, these are not the only FRs that can have biased results and, therefore, discriminatory effects, but they can be all of them. This situation is echoed in recital 54, which specifies that, for this reason, all RBIS (regardless of the time it takes to identify them) should be considered high risk. Generally speaking, the AIA establishes in many other recitals that AIs can lead to discriminatory situations in various contexts such as education or employment. More specifically, in the field of LEAs' actions (in this case, in a generic way, not directly linked to RBIS) situations may arise in which people are singled out in a discriminatory, incorrect or unfair way, especially when the instruments are not sufficiently transparent and explainable and are not well documented. It further adds where discriminatory results may come from, which may be caused by the mechanism not being trained with good quality data; not meeting adequate requirements in terms of performance, accuracy or robustness; or not being properly designed and tested before being introduced to the market.

3.1.Algorithmic discrimination

Prejudice and discrimination are risks inherent in all social and economic activity[654]. People tend to make decisions based on their own perception of the world and of others, i.e., driven by subjectivity. In general, there is a tendency to think that AIs are more adequate and reliable based on a presumption of greater objectivity because they are algorithms that act according to mathematical functions, i.e., under concrete and determined parameters. Despite this supposed objectivity, they can, as we have been pointing out, produce biased and erroneous results[655] that lead to discrimination against certain individuals or groups whose behaviour and daily life can be seriously affected[656].

[653] PELAIA, C. & NUCERA, G.G. "La prassi del *racial profiling* in Europa...", cit., p. 104.

[654] PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial...*, cit., p. 64.

[655] Therefore, adequate checks must be carried out before any investigative or law enforcement action is taken, in order to ensure public confidence that the police or security service is using the technology correctly and justifiably. LYNCH, N. "Facial Recognition Technology in Policing...", cit., pp. 6-7; & HOUWING, L. "Reclaim your face and the streets. Why facial recognition, and other biometric surveillance technology in public spaces, should be banned", in Quadflieg, S. et al. (Eds.), *(Dis)obedience in digital societies. Perspectives on the power of algorithms and data*, Transcript Verlag, Edinburgh, 2022, p. 330. The author is critical of the tendency to label algorithms as more objective when in fact they may reproduce existing biases and inequalities in society.

[656] The application of FRs by law enforcement has an impact on individuals or groups in a way that significantly affects the way they live in society and also impacts the democratic system, taking into

Moreover, it should be borne in mind that their effects are much broader than in the case of decisions taken by individuals, since they can affect society as a whole[657].

Discrimination in the algorithmic decision-making of FRs is not limited to a single moment, but can take place during design, testing and implementation, through the biases incorporated in the algorithm itself or the way in which the results are treated by the person or authority in charge of the system[658], even at the moment when police officers decide what action to take once a match has been produced[659]. Thus, from the moment the mechanism is created, discrimination may be favoured, even unintentionally. In this sense, the programmers of the system may have indirectly transferred discrimination from the analogical to the digital world. Not only that, but data may have been collected with erroneous or inaccurate methodologies that compromise the correspondence between the reality described by the aforementioned data and the real world; or it may also happen that the data have been obtained in an appropriate manner and are suitable for representing reality, but that reality is *per se* discriminatory, so that they are only capable of representing the discriminatory profiles existing in society.

In this sense, GERARDS argues that algorithms are not neutral, since those responsible for their design and application already have particular values and beliefs that will be transmitted to them, even unintentionally, and even databases are not neutral. Thus, we are dealing with instruments that are more characterized by subjectivity[660]. Similarly, in ODDENINO's opinion, the alleged neutrality and objectivity of data is a myth, given that if they represent society –subjectively– they will replicate the negative aspects that characterize it, especially the inequalities and discriminations that are perpetuated and consolidated over time[661], amplified in this case by the use of FRs. Along similar lines, COUCHMAN argues that these mechanisms can influence decision making and feed racial and socio-economic biases. Specifically, FRs are capable of massively misidentifying people of colour and are shown to be less likely to be accurate when used with trans and gender non-binary people, young people and women[662].

Thus, we are faced with a situation of algorithmic discrimination, understood as that which occurs when an individual or group receives arbitrary treatment as a result of automated decisions[663]. This can arise from the existence of biases in the training data as

account the great value of pluralism in it. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 8.

[657] PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial...*, cit., p. 65.

[658] MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU...*,*cit*., p. 7.

[659] FRA, *Facial recognition technology...*, cit., p. 27.

[660] GERARDS, J. "The fundamental rights challenges of algorithms," *Netherlands Quarterly of Human Rights*, vol. 37, nº. 3, 2019, p. 206.

[661] ODDENINO, A. "Intelligenza artificiale e tutela dei diritti fondamentali...", cit., pp. 191-194.

[662] COUCHMAN, H. "Mass Surveillance on Our Streets...", cit., pp. 587-588. The author argues that misidentifications affect not only underrepresented communities but also overrepresented ones. In both, discriminatory structures caused by surveillance appear, resulting in a form of state abuse that the FRs only exacerbate.

[663] MERCADER UGUINA, J.R. "Algorithmic discrimination and granular law: new challenges for equality in the era of big data", *Labos*, vol. 2, nº. 2, 2021, p. 6.

well as from the unequal distribution of variables such as gender or age; and from analytical defects derived from the lack of data, i.e., when these are incomplete[664] or of low quality[665].

But where do these discriminatory automated results derive from? In general, ML systems learn from the examples contained in the training set, so they tend to reproduce the flaws embedded in the training set[666], including the algorithm designer's own biases. Biases can occur even when the information from which it is fed does not include characteristics whose legal consideration is forbidden, such as gender or race. It may also happen that the training set is unfavourable to a certain group, resulting from an indirect discriminatory outcome. Errors may sometimes occur because of the use of data advantageous only to a particular group to the detriment of others; they may also result from distorted, biased human value judgments, or the examples in the training set may not reflect the statistical reality of the target population. The latter may be due to the fact that certain groups are subject to greater controls or less benevolent assessments, thus being more likely to be identified as perpetrators of undesirable behaviour, or because of the low representation of that group. All of the above is likely to lead to a significant reduction in the accuracy of forecasts and to reduce the attribution of desired characteristics and favour undesired ones[667].

In the case of FRs, what happens is that they learn to recognize people through the set of images used to train them and, if they have a larger number of photographs, they should theoretically produce more accurate results. However, accuracy depends not only

Algorithmic bias" is also referred to as systematic errors in a computer program that lead to unfair results. SCHUETZ, P.N.K. "Fly in the face of bias: Algorithmic bias in law enforcement's facial recognition technology and the need for an adaptive legal framework", *Minnesota Journal of Law*, vol. 39, nº. 1, 2021, p. 223.

[664] See, more extensively, MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal...", cit. Likewise, SORIANO ARNANZ alludes to these two ways in which algorithms can be biased. SORIANO ARNANZ, A. "Discriminación algorítmica: Garantías y protección jurídica", in Cotino Hueso, L. (Dir.), *Derecho y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, p. 140.

[665] The impact of poor data quality in IAs particularly strongly affects the right to non-discrimination, as highlighted by the FRA in *Data quality and artificial intelligence-mitigating bias and error to protect fundamental rights*, 2019, p. 8. On p. 2 of the same text, it further notes that an algorithm and its application can only be as good as the data it uses. In case these are of low quality the results will also be of low quality and this may lead to a violation of fundamental rights.

Recital 67 AIA also emphasizes the need for high quality and accessible data, as this provides structure and ensures the functioning of many AIs, especially when using techniques involving model training, with a view to ensuring that the high-risk mechanism works as intended and safely and does not become a source of any type of discrimination. To ensure data quality, appropriate data management and governance practices need to be put in place to ensure that the training, validation and test data sets are of high quality. Furthermore, these data have to be relevant and sufficiently representative, error-free and complete. Along with the above, they have to have adequate statistical properties, also with regard to the persons or groups with whom the system is intended to be used, trying to mitigate possible biases that may - among other things - have a negative impact on fundamental rights or lead to some kind of discrimination.

[666] Thus, as reflected in recital 67 of the AIA, biases may be inherent in the underlying data sets, especially when using historical data or data generated when systems are deployed in the real world. The results of IAs depend on such biases, which tend to increase gradually, perpetuating and amplifying existing discrimination, especially with respect to certain vulnerable groups.

[667] SARTOR, G. *L'Intelligenza artificiale e il Diritto...*, cit., pp. 72-73.

on the quantity of images processed but also on their quality, which requires representative datasets that reliably reflect the different population groups[668]. Thus, if the data contains more information on individuals belonging to a certain ethnicity or gender, it will be more accurate in that population set. Conversely, if another particular group is underrepresented, individuals belonging to that group run the risk of being misidentified[669]. In the countries around us, many mechanisms are trained primarily on data from white men, so it is expected that the systems will recognize them better than women and people of colour; and, in fact, this is the case. Research has shown that the technique has more failures in locating dark-skinned people and women, while the white male profile generates the fewest errors[670]. HOUWING has even described biometric surveillance technologies as racist and sexist because of their racial and gender discrimination[671].

Based on the foregoing, we can affirm that the social and racial biases that derive from FRs may contradict due process rights because those who have suffered negative consequences from misidentifications have greater obstacles to activate administrative remedies or access the courts to correct the error[672], which ties in with the violation of the right to the presumption of innocence[673] that we will address in the following section.

---

[668] FRA, *Facial recognition technology...*, cit., p. 27.

[669] RAPOSO, V.L. "Health, privacy and liberty...", cit., p. 535. Similarly, COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit., p. 129. The latter argues that companies have sometimes tried to remedy this problem by expanding the typology of data. Although this may appear to be an adequate solution, this modus operandi has been criticized because efforts should rather be directed at correcting problems of AIs that derive directly from the classification activity that is at the basis of the machine learning process.

[670] See, among others, INIOLUWA, D.R. et al. "Saving face: Investigating the ethical concerns of facial recognition auditing", *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, p. 146; THOMPSON, K.A. "Countenancing employment discrimination: Facial recognition in background checks", *Texas A&M Law Review*, vol. 8, nº. 1, 2020, pp. 64-65. On p. 67 the latter gives the example of Seattle police databases, in which photographs of African-Americans are more frequent because they tend to commit more crimes and, therefore, are arrested more frequently and are identified as false positives at a higher rate for criminal commission; SCHUETZ, P.N.K. "Fly in the face of bias...", cit. p. 223. The latter argues that the system identifies light-colored male features better than dark female features.

Specifically in the case of gender, BUOLAMWINI, J. & GEBRU, T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, vol. 81, 2018, pp. 1-15.

[671] HOUWING, L. "Reclaim your face and the streets...", cit. p. 330.

Thus, in view of the fact that it is a technique that favours racist bias, some large multinationals that sold their FR products to law enforcement, including IBM and Amazon, withdrew them from the market. NAVARRO, B. "IBM y Amazon abjuran de la tecnología de reconocimiento facial por su sesgo racista", *La Vanguardia*, 16 June 2020. Electronic resource obtained via the Web: https://www.lavanguardia.com/internacional/20200611/481710398480/ibm-reconocimiento-facial-racismo-tecnologia-negros.html, [retrieved 2 August 2024].

[672] RAPOSO, V.L. "Health, privacy and liberty...", cit., p. 535.

[673] In this regard, we bring up the 2021 arrest of an African-American individual in the city of Detroit (USA) for a crime he had not committed. He was identified by means of an old photograph on his driver's license. As a result, he had to face legal proceedings even though he insisted on his innocence. Fortunately, the Prosecutor asked for acquittal due to lack of evidence. LABORDE, A. "Detenido injustamente un afroamericano en EE UU por un error en el sistema de reconocimiento facial", *El País*, 26 June 2020. Electronic resource obtained through the Web: https://elpais.com/tecnologia/2020-06-26/un-afroamericano-es-detenido-injustamente-por-un-error-en-el-sistema-de-reconocimiento-facial.html, [retrieved 1 August 2024].

Thus, individuals unjustly identified and accused as those targeted by LEAs suffer algorithmic discrimination.

In line with what we have just indicated, and following SORIANO ARNANZ, the fact that an algorithm contains or develops generic biases does not imply *per se* that it causes discrimination, but rather that the risk of perpetuating the disadvantage of marginalized groups occurs if the algorithm commits errors[674] as a result of the biases it contains. Thus, the latter do not act directly as a source of discrimination, but rather as an effect that may derive from the existence of biases in the datasets with which the system operates.

As a result, and by way of summary, the collision of FRs with the right to non-discrimination focuses on two main issues. On the one hand, the disproportionate impact of technology against certain groups and, on the other, its low accuracy[675], derived from the existence of biases. It is important to highlight that ocular identification by individuals is significantly less reliable than FRs, which perform this task much better. For this reason, SARTOR believes that, although algorithmic systems may reproduce or increase the existing inequality, the processes they follow to deliver a given result are more controllable than human decisions. Therefore, he understands that the future challenge is to find the best combination between AIs, in our specific case, those based on the FR, and human intelligence[676].

3.2.Direct and indirect algorithmic discrimination

Algorithmic discrimination, like any other type of discrimination, can be of two types: direct and indirect. The first occurs "where one person is treated less favourably than another is, has been or would be treated in a comparable situation"[677], while the second takes place "where an apparently neutral provision, criterion or practice would put persons having a particular religion or belief, a particular disability, a particular age, or a particular sexual orientation at a particular disadvantage compared with other persons"[678].

[674] SORIANO ARNANZ, A. "Discriminación algorítmica...", cit., p. 141. Similarly, ZUIDERVEEN BORGESIUS, F.J. "Strengthening legal protection against discrimination by algorithms and artificial intelligence...", cit., p. 1575, when he argues that algorithms are not inherently bad or discriminatory and, if necessary, could even contribute to reduce discrimination.

[675] LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit. p. 6.

[676] SARTOR, G. *L'Intelligenza artificiale e il Diritto...*, cit., pp. 74, 75.

[677] Articles 2.2.a) Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin; and Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

[678] Articles 2.2.b) Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin; and Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

Direct discrimination involves an explicit distinction of individuals or groups[679]. In the case of algorithms, it would be intrinsic with respect to the source code as it was conceived, leading to discriminatory decisions. Thus, this typology is concerned with protecting formal equality insofar as it focuses on ensuring that no decision privileges a particular group or individual over others[680]. Such a form of inequality is prohibited because the decisional process of the algorithm cannot be based on directly discriminatory parameters[681]. In order to know whether we are dealing with direct algorithmic discrimination, it is necessary for the system to process a category of data and consider the individual's membership of a disadvantaged subgroup and that this is taken into account to make the decision, or else that the individual's membership of this group is inferred. Thus, it would be understood as the application of negative stereotypes to protected groups[682] through automated mechanisms. Extrapolating it to the way FRs operate, direct discrimination would take place, for example, when the algorithm is designed to identify individuals belonging to certain minority groups, as happens in China with the Uyghur population, as indicated above.

Such discrimination is easy to prove when the source code is not accessible and all members of the same group are affected. Conversely, if only one individual is affected, it would be more difficult to identify. It is also complicated when there is no possibility of accessing information about the decision and how it was made, as this hinders the possibility of establishing a valid comparative reference. In the case of algorithms that act as a black box, it is even worse, since if they have been designed by a private company, there may be intellectual or industrial property protection and trade secrets[683], making it very difficult, if not impossible, to access this information. This situation makes it difficult to know how the algorithm works and what data it contains, and therefore whether it discriminates directly.

Indirect discrimination, which is the effect of a certain practice and does not derive from the direct action of the individual or mechanism[684] and comes from factors that cannot be immediately traced back to the code, is different. It is more diffuse but much more frequent than the previous[685]. It is usually unintentional and is caused by the handling of unrepresentative training data, biases in data labelling schemes and faulty or

[679] The elements that have to be present in a specific situation in order to understand that there is direct discrimination are: 1) less favourable treatment; 2) with respect to another person who is in a similar situation; and 3) that this different treatment is based on one of the protected grounds provided for in European anti-discrimination law (gender, sexual orientation, disability, age, race, etc.). FRA, *Handbook on European non-discrimination law*, 2018, pp. 47-58.

[680] SORIANO ARNANZ, A. "Algorithmic Discrimination...", cit., pp. 145-146.

[681] COTINO HUESO, L. "Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection...", cit., p. 361.

[682] SORIANO ARNANZ, A. "Discriminación algorítmica...", cit., p. 149.

[683] *Ibd.*, p. 154.

[684] ZUIDERVEEN BORGESIUS, F.J. "Strengthening legal protection against discrimination by algorithms and artificial intelligence...", cit., p. 1577.

[685] *Idem*. The concept of indirect discrimination itself does not provide a clear and concise rule as to what is meant by it. For that reason, it gives rise to rather open standards that are often difficult to apply in practice.

inadequate mathematical functions[686]. The FRA defines it as occurring when an apparently neutral arrangement introduces a disadvantage to an individual or a group of individuals who share the same characteristics. In order to establish this disadvantageous treatment, it must be shown that a group is disadvantaged by a decision with respect to the reference group[687]. In this case, discrimination of this kind could occur when the decisions taken may seem legitimate and the victim has no feeling of being discriminated against. This may be due to the way in which the FRs operate or the decision or result they issue, which give an appearance of false neutrality but, in reality, are discriminatory, in the sense of disadvantaging individuals or groups because of some protected characteristic. This results in erroneous outcomes in a way that further disadvantages those groups in a disguised or not directly discriminatory way.

Thus, we understand that it is necessary to ensure that both types of discrimination are eliminated from the FRs, given that their installation in uncontrolled spaces entails the possibility of detecting on a large scale an indefinite number of individuals who, if incorrectly identified due to the biases contained in the mechanism, may be victims of discriminatory treatment and, therefore, this fundamental right is massively violated.

3.3.Errors and biases

As already indicated, AIs and, by extension, FRs do not give absolute results, but rather in terms of probability. This, together with the existence of biases in the databases or the fact that they contain some type of erroneous personal information, can lead to incorrect identifications, in addition to the possible inappropriate use of the mechanisms[688]. As a result, innocent citizens may be the subject of a police investigation[689].

---

[686] COTINO HUESO, L. "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos...", cit., p. 361.

[687] FRA, *Handbook on European non-discrimination law...*, cit., p. 58. The elements of this type of discrimination are set out on pp. 60-66, and are: 1) existence of a neutral provision, criterion or practice; 2) that it produces more detrimental effects for a protected group; 3) in comparison with a reference group. For this, the existence of both groups, the one at an advantage and the disadvantaged one, must be proven.

[688] BREY, P. "Ethical aspects of facial recognition systems in public places...", cit. p. 104.

Bias does not always refer to a negative concept, since it is a way in which the human brain processes information. Thus, gender bias, for example, is one of the judgments made by the brain that influences our decisions and is based on perceptions of gender gained from our cultural experiences and social beliefs. In the event that unwanted preferences are created against a particular group because of its particular attributes, discrimination in a negative sense is produced, and such prejudices are reproduced daily until they produce a type of systemic discrimination that permeates society. MUNARINI, M. "New perspectives on the mitigation of gender bias in AI by EU regulations...", cit., p. 118.

[689] It happened in 2001 in the city of Tampa, Florida. Milliron was eating lunch in a public area when his image was taken by an FRs and he was arrested by the police. His image appeared in a newspaper article about the technique in which his image was included along with those of other individuals. A lady in Oklahoma identified him (also mistakenly) as her ex-husband who had child neglect charges. However, this individual, who had never married and never had children, stated that "they mad me feel like a criminal". This led KOPEL/KRAUSE to describe the technique as humiliating and ineffective. KOPEL, D.

Errors arising from FRs are of two types: false positives and false negatives[690]. The first involves the incorrect identification of an individual as one of the persons included in the watchlist when in fact he or she is not, while the second occurs when the mechanism fails to detect a subject who is included in the same[691] and, therefore, is the object of a police search. The system is not infallible and can be manipulated to avoid detection[692]. This is very simple as wearing certain accessories can block certain key areas of the face or cast shadows on them, making it unrecognizable by the system[693]. Moreover, some methods have been designed to circumvent the facial recognition mechanism through concealment or confusion[694]; and some techniques have been developed to confuse video surveillance cameras. One of them is based on the creation of images of different colours that can be printed and used in the real world, hiding individuals from the detectors, suggesting that the systems could be easily vulnerable to

& KRAUSE, M. "Face the facts: facial recognition technology's troubled past-and troubling future", *Reason*, vol. 34, nº. 5, 2002. The authors expose more cases of misidentifications through FRs and the negative consequences that resulted.

Other more recent examples of system failures can be found in SCHUETZ, P.N.K. "Fly in the face of bias...", cit. pp. 233-236.

[690] In the field of crime prediction in general, a false negative occurs when the system erroneously allows a guilty individual to escape, while false positives occur when an innocent person is suspected of being guilty. MILLER notes an essential problem in the latter, and that is the phenomenon called "base rate fallacy", which emerges when a large number of "normal" profiles are scrutinized but the incidence of the target profile is very small. Even in a large population, a model that is considered accurate will result in few matches. MILLER, K. "Total surveillance, Big data, an predictive crime surveillance...", cit., p. 121. The problem is that it is accepted at the institutional level that the systems have an error rate. Thus, the author states that the FBI considers it acceptable for its Next Generation Identification biometric program to make incorrect matches 20% of the time. He goes on to state on pp. 122-124 of the same research that people's trust in machines promotes biases and, consequently, he argues that there is an initial tolerance for false positives and negatives.

[691] FRA, *Facial recognition technology...*, cit., p. 9. The Agency establishes three important considerations on this issue: 1) an algorithm never gives a definitive result, only in terms of probability; 2) as a consequence, there is always a trade-off between false positives and negatives because of the decision on the probability threshold; and 3) the rates must be evaluated taking into account the number of real cases.

[692] This situation is not unique to FRs and is common to all biometric recognition systems which, despite being more efficient compared to traditional measures, are vulnerable to adversarial attacks. This is because DL and ML mechanisms are exposed to these new vulnerabilities. They are usually imperceptible modifications to the original data that alter them and carry serious threats in the sense of undermining the reliability and integrity of the systems. ALGHAMDI, S.M. et al. "Enhancing security in multimodal biometric fusion: Analyzing adversarial attacks", *IEEE Access*, vol. 12, 2024, p. 2.

[693] LEARNED-MILLER, E. Et al. *Facial recognition technologies in the wild: A call for federal office*, MacArthur Foundation, 2020, p. 10.

Similarly, cosmetic surgery, by making modifications to the face, is likely to alter the recognition of individuals. As this practice is widespread today, it poses a challenge for FRs. GABOR, T. et al. "Robust thermal face recognition for law enforcement using optimized deep features with new rough sets-based optimizer," *Journal of Information Security and Applications*, vol, 85, 2024, p. 2. To prevent the system from failing to adequately detect both individuals who have undergone cosmetic operations and other ways of altering face parameters, the authors propose a mechanism that combines illumination, expression, and surgical invariance to provide a robust recognition method. They designed it by extracting strong facial features and then selecting the most discriminative features while reducing computational cost and maintaining high accuracy. For further discussion, see pp. 1-17.

[694] MERINO, M., "Estos son los métodos con los que intentan sortear el reconocimiento facial los defensores de la privacidad", *Xataka*, 10 April 2019. Electronic resource retrieved from World Wide Web: https://www.xataka.com/inteligencia-artificial/estos-metodos-que-intentan-sortear-reconocimiento-facial-defensores-privacidad, [retrieved 2 Aug 2024].

this type of attack[695], making it difficult or impossible to identify people who are the object of police search, thus causing false negatives. In addition, the mechanism can be tampered with if someone who does not have access to it impersonates the user and deliberately manipulates its biometric trace to avoid detection[696].

In view of the above, false positives are more dangerous because of their legal implications and the consequences they entail[697] for those who have been incorrectly identified as dangerous criminals or terrorists, or suspected of committing a possible serious crime, because a match has been made with the information contained in a watchlist and proceedings have been initiated against them.

The level of probability of hit and miss is based on the accuracy of the system, i.e. the number of false positives and negatives it emits, which in turn depends on the technique used. Although this is a technical rather than a legal aspect, the level of accuracy of the mechanism must be specified when used in the field of law enforcement, since an incorrect identification can lead to arrest (in the case of erroneous, illegal identifications) and public disclosure of personal identity, bringing social discredit and damage to reputation[698].

If we add to this the biased results that, as we indicated, can be produced in many ways, a situation of discrimination can be created[699]. The representativeness of a population set is also critical to avoid errors, as individuals belonging to groups that are

[695] THYS, S. VAN RANST-W. & GOEDEMÉ, T. "Fooling automated surveillance cameras: Adversarial patches to attack person detection", *arXiv.org*, (Cornell University Institutional Repository), New York, 2019, pp. 5-7. The authors of the technique believe that if combined with a sophisticated clothing simulator, a T-shirt could be designed that could render the person invisible to automated surveillance cameras.

The EDPB also refers to the ease with which the system can be fooled, for example, with images of fake faces, which is known as "spoofing". EDPG, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 13.

[696] JAIN, A.K. et al. "Biometrics: A tool for information security", *IEEE Transactions on Information Forensics and Security*, vol. 1, nº. 2, 2006, p. 131. 133 the different ways in which attacks can occur: 1) *cicumvention:* an intruder would fraudulently gain access to the system by bypassing the biometric comparator and examining the data, which he can then modify; 2) *repudiation*: the legitimate user can access the facilities offered by an application and then claim that an intruder had circumvented the system. Thus, he is able to modify information and subsequently deny responsibility; 3) *collusion*: an individual with administrator privileges can deliberately modify biometric system parameters to allow incursions by an intruding collaborator; 4) *coercion*: an imposter can force a legitimate user to grant him access to the system; and 5) *denial of service*: an attacker can overwhelm system resources to the point where legitimate users are denied access. For example, it could act by processing bogus access requests, overloading computational resources and preventing valid requests from being processed.

[697] MITCHELL, A. "Distinguishing friend from foe...", cit., p. 300. The author points out that one of the causes of error may come from the fact that there is no biometric characteristic that is completely stable and distinctive since a biometric sample is not always the same. As ZUIDERVEEN BORGESIUS states, false positives are a big problem in the field of criminal law because it can lead to your arrest, detention, etc. And he asserts that we should not accept algorithmic decisions that violate the underlying values of criminal law. ZUIDERVEEN BORGESIUS, F.J. "Strengthening legal protection against discrimination by algorithms and artificial intelligence...", cit. p. 1585.

[698] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., pp. 527-528.

[699] MOBILIO, G. "Your face is not new to me...", cit. p. 17.

less represented in the algorithm's training set are more prone to misidentifications[700] and this can have repercussions, we reiterate, on a large scale[701] when FRs are used because, even with a minimal error rate, the false positive rate in uncontrolled environments is very high, causing authorities to misdirect their attention to certain categories of people, namely those who are most frequently identified by the mechanism even if incorrectly.

In order to avoid false identifications due to the existence of insufficient training databases and poor quality or veracity of those, obligations related to quality management and data governance must be implemented in all phases of the system, with transparency and explainability being fundamental[702]. The latter is very difficult because the mechanism often acts as a sort of black box that makes it very difficult to obtain full knowledge of it.

3.4.Black boxex

FRs are usually based on complex DL mechanisms that operate through the analysis of large amounts of data in a very fast time and allow unpredictable decisions to be taken even for the programmers themselves. They are software that act with a remarkable level of opacity, being a black box[703]. All this can make it difficult to detect possible violations of the normative provisions designed to protect fundamental rights, to determine responsibility, to impose sanctions and to satisfy the demand for compensation[704].

---

[700] LEARNED-MILLER, E. et al. *Facial recognition technologies in the wild: A call for federal office*..., cit., p. 9; & CHOWDHRY, A. et al. "The pitfalls of surveillance technology: Policy analysis and solutions", *Institute for Youth in Policy. Policy Department I Brief*, 2023, p. 1. The authors indicate that six out of seven cases of misidentifications are of people of colour. Because of this high percentage, they call for a ban on the technology.

[701] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 528; SCHEPISI, C. "Diritti fondamentali, principi democratici e *rule of law*...", cit., p. 216.

[702] COTINO HUESO, L. "Automated facialrecognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection...", cit. pp. 390-391. To avoid biases and errors, system managers have to check the quality of the images and templates inserted in watch lists to avoid possible false matches. In addition, they have to be able to establish the performance requirements and express them appropriately.

[703] The term "black box effect" is normally used to express human uncertainty about the technological system when biases, unknowns, complexity and secrecy combine to the point of making the mechanism incomprehensible. Thus, it is very difficult to understand how it has arrived at a certain result, because its internal processes are impenetrable and opaque. They can arise at all stages of the process (from instrument design through implementation and maintenance to maintenance). In addition, black boxes contribute to the problem of algorithmic biases. MILLER, K. "Total surveillance, Big data, an predictive crime surveillance...", cit., pp. 136-137. However, we should clarify that not all ML algorithms operate as black boxes, as decision trees, Bayesian classifiers, additive models, etc., use a reasonably restricted number of internal components, which provides traceability and transparency in their decision making. RAI, A. "Explanaible AI: From black box to glass box", *Journal of the Academy of Marketing Science*, vol. 48, 2020, p. 138.

[704] DONATI, F. "Diritti fondamentali e algoritmi...", cit, pp. 112-113.

As we have indicated above, all intelligent systems operate with a certain margin of error, which is highly detrimental in the case of those targeting large populations as is the case with FR, as it contributes to facilitate discrimination. For this reason, a much higher level of precision is required. What happens is that the more accurate the analysis performed by the AI, the more difficult it is to get an explanation of why the machine has made a decision[705].

When systems are based on complex DL and ML algorithms, the way in which they operate and learn becomes much more independent and opaque, which makes them difficult to understand[706] and, when it comes to DNN, the intermediate phases of the decision-making process are hidden from people due to the technical complexity that surrounds them[707]. This is because the mechanism is made up of different levels or layers, and the more layers there are, the more difficult it is to get to know the process followed to reach a certain result, making it difficult to know and mitigate the vulnerabilities of the system and the biases[708]. Therefore, the latter will continue to be perpetuated, as will the discrimination that results from them, if it is not possible to know how the algorithm works and the data from which it is fed[709], in order to evaluate its quality and whether it is representative of all the social groups in the population in which the system is implemented.

The effectiveness of the algorithmic process of data control must necessarily contemplate mechanisms that guarantee the correct establishment of a minimum and informed contradiction between person and machine, in the sense that those involved have the right to know the mathematical and statistical rules that are included in the automated decisional process that affects them. In this way, respect for the principle of transparency would be guaranteed, in the sense that the interested party has all the information necessary to understand the way in which a particular decision concerning him has been

[705] TSCHIDER, C.A. "Beyond de 'black box'", *Denver Law Review*, vol. 98, nº. 3, 2021, p. 688; VALLS PRIETO, J. "Derecho penal y la inteligencia artificial: Una metodología de análisis", in Peralta et al. (Coords.), *El Derecho y la Inteligencia Artificial*, EUG, Granada, 2022, p. 507.

[706] GERARDS, J. "The fundamental rights challenges of algorithms...", cit., p. 206.

[707] ZAVRSNIK, A. "Criminal justice, artificial intelligence systems, and human rights...," cit., p. 568.

[708] MILOSSI, M. "Remote biometric identification systems and ethical challenges...", cit., p. 4. On the contrary, decision trees are completely intelligible and act as a sort of "white box" that allows to know the process by which a conclusion has been reached. SALAZAR, I. "El diseño ético de la inteligencia artificial para no discriminar ni lesionar derechos", in Balaguer Callejón, F. & Cotino Hueso, L. (Dirs.), *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, Zaragoza, 2023, p. 91.

An explainable IA provides the appropriate details to make its operation clear or easy to understand. This may be through a white box model or subsequent explainability techniques. The ultimate goal, whatever the model, is to boost the transparency of the solutions and the ability to trust the results of the system. HERRERA, F. et al. "Una visión actual de la Inteligencia Artificial...", cit. p. 73.

[709] ZUIDERVEEN BORGESIUS, F.J. "Strengthening legal protection against discrimination by algorithms and artificial intelligence...", cit. p. 1577. The author refers mainly to indirect discrimination, since it is more difficult to observe than direct discrimination and systems that operate with black boxes do not contribute to its clarification.

taken[710]. Similarly, PRESNO LINERA considers it essential to know the black boxes that hide the use of AIs as an additional guarantee of transparency[711]. However, this is difficult to achieve because the systems can be opaque, either because of a business choice (since most instruments are created by private companies) or because of technical reality, i.e., companies could decide to keep secret certain information such as the infrastructure of the mechanisms and the methods by which the algorithm has been created, protecting the intellectual property of the algorithm. Moreover, the algorithm itself may be technically inscrutable[712]. Thus, it is practically impossible to achieve complete transparency.

Some authors are critical of the demand for transparency of the algorithm or full access to the source code *strictu sensu*, such as SIMÓN CASTELLANO, who refers to this phenomenon as a "fallacy of transparency" and understands that it is not a question of having access to the algorithmic code or of its design and logic being transparent (since, we add, even so, due to the technical characteristics of the systems, it will be very difficult for an ordinary citizen lacking technical knowledge to understand the mechanism's operation), but rather that people should not be the object of an automated decision without human intervention from which legal effects are derived and from which they cannot defend themselves or react with guarantees in the face of it. Along these lines, it alludes to the provisions of art. 22.3 GDPR, in the sense that the individual has the right to the intervention of the person responsible for knowing the logic of the code and accessing it, in order to help ensure that no one is subject to an exclusively automated decision[713] and thus facilitate the understanding of the result to which he or she has been subjected. The necessary human intervention in automated decision-making processes constitutes one of the new rights that have appeared with the advance of AIs, which will be discussed below in the corresponding section of this research.

Thus, the need to eliminate biases that can lead to erroneous results (in our case, false identifications through the FRs) and thus perpetuate discriminatory situations against certain social sectors –either directly or indirectly– means that the data and decision-making procedures must be made public and can be subjected to technical evaluations that allow these results to be questioned. However, ensuring transparency through access to information is complicated, not only because of the black boxes, but also for other reasons. On the one hand, some information is inaccessible to victims because it is proprietary or the company that created the algorithm invokes intellectual

[710] RICCIO, G.M. & GIANNONE CODIGLIONE, G. "La rilevanza delle basi giuridiche per il trattamento di dati personali mediante sistemi di intelligenza artificiale...", cit. pp. 310-311.

[711] PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial...*, cit., p. 91. There are ways to transform black boxes into glass boxes. For more on this process, see RAI, A. "Explanaible AI...", cit., pp. 137-141.

[712] TSCHIDER, C.A. "Beyond de 'black box'...", cit., p. 700. The author points out that the black box problem originates when the opacity of the algorithm impacts on individuals.

[713] SIMÓN CASTELLANO, P. "Allende una teoría general de las garantías para una inteligencia artificial confiable", in Balaguer Callejón, F. & Cotino Hueso, L. (Dirs.), *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, pp. 115-117. In spite of the above, the author does not consider that transparency is not necessary, but that it is one more extreme of all the guarantees that AIs have to observe.

property rights. On the other hand, the courts may also refuse to make data concerning the data subject available to them. So, without knowledge of at least the result that has been reached, the data subject could find it very difficult to determine whether he or she has been the victim of discrimination[714]. It is necessary to eliminate –or at least reduce– all the obstacles that hinder access to information on the way in which the system has made a decision, which would facilitate understanding of the system, of the algorithm with which it works, and would also make it possible to know the data it uses in order to know whether it is of good quality and whether it contains any type of bias. By analysing all this, it would be possible to work to correct the aspects that favour identification failures and avoid discrimination.

4. Presumption of innocence and other rights in the field of criminal law

The rights to effective judicial protection and the presumption of innocence are included in arts. 47 and 48 of the Charter, respectively. Both are endangered by the inclusion of the FRs in the different phases of the criminal procedure[715]. However, despite the interest in studying the former, we will focus mainly on the latter, since it is one of the most important safeguards that citizens have against the punitive power of the State and is especially affected in this initial phase of the police investigation in criminal matters.

According to this right, no one can be found guilty until a final sentence has been handed down in which responsibility for the acts attributed to them is established. In this way, the presumption of innocence is seriously compromised by the use of FRs and the danger of mass surveillance that they entail, given that all citizens are presented as potential suspects[716], in addition to the fact that they can be subject to police surveillance without any suspicion or search warrant[717], to which is added that the results issued by the algorithm are capable of acting as decisive evidence in the judicial process[718].

In a state governed by the rule of law, citizenship is presumed to be fair until proven otherwise[719]. However, there is a risk that the results of the instrument are imposed independently of the individual conduct of the subject or his personal circumstances, because they are based solely on a match of the image of the person with those contained in a watchlist. In addition, the burden of proof is reversed and passes to the accused, who

[714] MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU...*, cit., p. 20.

[715] In this regard, see more extensively, NOVOKMET, A. et al. "Facial recognition technology in EU criminal justice...", cit., pp. 557-562.

[716] GATES, K.A. *Our biometric future...*, cit., p. 94; Cas, J. et al. "Introduction. Surveillance, privacy and security...", cit., p. 7.

[717] KINDT, J.E. "Having yes, using no?", cit., p. 528.

[718] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 15.

[719] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 1.0*, May 12, 2022, p. 46.

must prove his innocence, because when the system identifies an individual as one of those collected in that database, his guilt is presumed –even if a false positive has been committed– by normally granting a very high degree of credibility to the mechanism[720] on the basis of the supposed objectivity already mentioned above.

There is thus a shift from a presumption of innocence to one of guilt because the suspects, especially those who have been incorrectly identified, are the ones who have to prove their innocence, whereas the accuser normally has to prove their guilt[721]. So they have a higher burden to prove that they are innocent and will have to prove that they are not who the mechanism says they are and that, therefore, the match was wrong[722]. In a different sense, NOVOKMET et al. understand that, because the instrument issues the result in percentage terms, the defendant has a strong argument to challenge a decision that does not favour him[723]. However, in practice this is not the case, and when the FRs identify a person, he is presumed guilty and must prove that he is not, thus altering the principle of the presumption of innocence. Not only is there a reversal of the burden of proof, but also the stigmatization of individuals to the extent that they are considered as suspects of having committed an offense when in fact they were innocent[724].

On the other hand, and linked to this, mass monitoring through FRs also interferes with the principle of reasonable suspicion to initiate criminal proceedings. This is because the introduction of such systems in conventional CCTV and video surveillance cameras results in constant monitoring that is not initiated on the basis of such suspicion, but is generated through the analysis of the data produced by the mechanisms[725]. Thus, it elevates millions of people to the rank of potential suspects even in a narrow field of investigation.

In this sense, the Judgement CJUE (Grand Chamber) 8 April 2014, Joined Cases C-293/12 and C-594/12, in paragraphs 58 and 60 expresses that there is no limitation of the persons to whom the measure is addressed (in this case of electronic communications and users who use such services, although it can be extrapolated *mutatis mutandi* to the state of surveillance that would cause the FRs) reaching individuals who are not even

[720] PÉREZ TRENCH, N. "Los sistemas de reconocimiento facial...", cit., p. 75.

[721] However, this does not prevent the accused from requesting that the Public Prosecutor's Office investigate certain facts, require certain elements and evidentiary bodies to disprove the prosecution's thesis of guilt. AMONI REVERÓN, G.A. "Libertad, presunción de inocencia y defensa...", cit., p. 211; PÉREZ TRENCH, N. "Los sistemas de reconocimiento facial: Una mirada a la luz del examen de proporcionalidad", *Revista Internacional de Derechos Humanos*, vol. 12, nº. 1, 2022, p. 75.

[722] MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU...*, cit., p. 7.

[723] NOVOKMET, A. et al. "Facial recognition technology in EU criminal justice...", cit., p. 553. They go on to point out that the situation is more complicated in cases where the percentage is lower as it puts on the borderline whether the individuals have the status of citizen or suspect.

[724] GALETTA, A. "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?", *European Journal of Law and Technology*, vol. 4, nº. 2, 2013 (unpaginated).

[725] MURRAY, D. & FUSSEY, P. "Bulk surveillance in the digital age...", cit., p. 47. The authors go on to note that these practices of mass communication and security through technological surveillance raise serious questions about the role of probable cause and reasonable suspicion, along with issues related to due process and the presumption of innocence.

indirectly involved in a situation that may result in criminal prosecution. Therefore, it extends to the citizenry as a whole, since, as reflected in the pronouncement, it reaches individuals with respect to whom there are no indications suggesting that their conduct may be related to serious crimes. Thus, it may involve a great interference in fundamental rights, in this specific case, the presumption of innocence.

The ECHR has ruled on the processing of biometric data and the right we are analysing in this point in the oft-cited judgement *S. and Marper v. The United Kingdom*. There, the applicants (see para. 89) emphasized that the retention of biometric data records for an indefinite period of time gave rise to the suspicion that, even if a person has been acquitted, he or she is not considered to be totally innocent. Furthermore, they argue that this results in the stigmatization of individuals belonging to ethnic groups that are more overrepresented in the database. The Court, in para. 122, links the latter to the presumption of innocence. It holds that the latter is a right whereby one who has not been convicted of any crime is entitled to have no suspicion of innocence expressed until after the accusation has been verified. This being so, although he argues that the retention of the data cannot be equated with the expression of suspicion, the claimant's perception that they are not being treated as innocent is reinforced if the data is retained indefinitely as is done with those who are convicted.

As a result, the indefinite storage of biometric data in a database does not imply the violation of the presumption of innocence, but what it may cause is a feeling in individuals of being subjected to different treatment for that reason. It is a different matter if one is identified by biometrics as a suspect in a crime. Such a situation would suggest that the individual whose personal data, such as facial image, fingerprints, DNA, etc., have been linked to those contained in a police database is indeed guilty of the crime for which he is being prosecuted. Therefore, he will have to face the action of proving his innocence and verifying that who the system says he is does not coincide with reality.

In the case of FRs, especially those that act in real time, agents must be cautious and assess the veracity of the data, otherwise they could result in immediate arrest and the initiation of criminal proceedings, seriously jeopardizing not only the presumption of innocence but also all the other fundamental rights and freedoms that we have been analysing so far. The exercise of these rights is not absolute and can be limited[726] under certain strict circumstances that we will have the opportunity to study later.

[726] This does not extend to the right to the presumption of innocence, since its elimination would render the process useless because if the person is already considered guilty beforehand, the criminal process would be useless. AMONI REVERÓN, G.A. "Libertad, presunción de inocencia y defensa...", cit., p. 221.

5. New rights on the digital field

Not only traditional rights are affected, because other new rights deserving protection may arise, not even foreseen in the Charter[727], linked to the constant development and evolution of AI. In line with the above, it should be noted that the particular characteristics of these mechanisms demand that any regulatory scheme that intends to regulate them be sufficiently flexible to adapt to the changes caused by them, since the continuous evolution of technological applications runs the risk of rendering obsolete any regulation[728] that is more or less rigid. The anthropocentric approach of the AIA leads to affirm the need to consider all the rights included in the Charter as the basis for establishing the standard of protection, serving as the normative basis and international standard of the anthropocentric AI[729] . Thus, alongside the traditional rights, some new rights are already appearing, typical of the new digital society created by the development and expansion of intelligent systems[730].

5.1.Human intervention in aumatic decision-making processes

Among these rights is that of human intervention in automated decision-making processes, provided for in art. 22 GDPR. Its content refers to the right of individuals not to be subject to a decision based solely on automated processing. The High-Level Expert Group on AI established in the *Ethics Guidelines for Trustworthy Artificial Intelligence* the action of human oversight as one of the ethical principles that all AIs must observe. This is because such mechanisms are tools at the service of people that must respect human dignity and personal autonomy, functioning in such a way that they can be adequately controlled and monitored by human beings.

Similarly, the Europe Council in 2019 in Step 9 to protect AI human rights[731], stated that all AIs should be controlled by individuals, even when the mechanisms make decisions independent of specific human intervention. It further adds that Member States should provide access to an effective remedy for those who suspect that they were subjected to an action taken solely by an AI in a non-transparent manner and without their knowledge. To the above, it adds that they must guarantee the right for citizens not to be

[727] ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione...," cit., p. 148.

[728] ODDENINO, A. "Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, p. 170.

[729] This approach is criticized by ODDENINO for whom this logic is excessively generic, has some limits of effectiveness for the protection of fundamental rights because the risk-based approach is incomplete and does not adequately consider algorithmic discrimination. *Ibd*., pp. 199-200.

[730] ADINOLFI lists those that he considers are currently emerging. See, ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione...", cit. pp. 150-152.

[731] Europe Council, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights...*, cit.

subjected to a decision that significantly affects them based solely on an automated decision-making process without human intervention and also that they can obtain such intervention and have the views of individuals taken into account before the decision is implemented.

Likewise, the AIA takes this requirement into account in several recitals. Thus, for example, in number 73, specifically in the case of RBIS, it considers it necessary to establish it in a reinforced form, so that the person responsible for the system cannot act or make decisions based exclusively on a result of the system until at least two natural persons have verified and confirmed it separately. It remains to be seen whether, with the development of technology, this right will be guaranteed or whether, on the contrary, for reasons of speed in decision-making, decisions will begin to be taken without human supervision, thereby infringing this right.

5.2.Right to be forgotten

This new right is linked to privacy and some of its aspects related to individual autonomy. The right to be forgotten is seen as an understandable reaction to the widespread penetration of ICTS in our lives[732]. It is especially relevant in the case of the Internet and is based on the fundamental need of an individual to determine the development of his or her life autonomously without being perpetually or periodically stigmatized as a consequence of a specific past action in this environment, especially when such action took place many years ago and no longer bears any relation to the current context[733]. It is linked to the idea of forgetfulness as the subjects' control over their past in this environment in relation to facts and situations that are real and appropriate but which they would prefer not to be accessible by others[734]. In this sense, the CJEU Judgement, C-131/12 of 13 May 2014, case *Google Spain v. Spanish Data Protection Agency,* deals with it extensively albeit from the perspective of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It did not expressly mention this right, which is why the data subject was not entitled to restrict or stop the dissemination and use of personal data that he or she considered harmful or contrary to his or her interests. However, the GDPR does establish this right to be forgotten in art. 17. Personal data must cease to be processed and

[732] YUDKIVSKA, G. "New approach to the right to privacy in times of transparency and mass surveillance", in Sturma, P. et al (Eds.), *70th Anniversary of the European Convention on Human Rights*, Rw&w Science & New Media, Bayern, 2021, p. 47.

[733] MANTERELLO, A. "The EU proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'", *Computer Law & Security Review*, vol. 29, 2013, p. 230.

[734] SUSI, M. "The & right to be forgotten", in Von Arnauld, A. et al. (Eds.), *The Cambridge Handbook of new human rights. Recognition, novelty, rhetoric*, Cambridge University Press, Cambridge, 2020, p. 287; ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales...*, cit., p. 247.

be deleted without undue delay when they are no longer necessary for the purposes for which they were collected or otherwise processed; the data subject withdraws consent or objects to the processing; and the personal data have been processed unlawfully.

The right to be forgotten aims to balance privacy and freedom of expression on the Internet. Moreover, it is based on the idea of personal autonomy and the ability to control one's own personal data for the purposes of self-determination[735]. On the other hand, it should be specified that this right is different from the right to data deletion described in previous sections, since the latter applies to information that is not real or adequate. On the other hand, this right arises immediately after the information has been made publicly accessible and the affected party has the right to request its deletion or rectification. If it is observed that it does not meet the criteria of adequacy and truthfulness, the operator has the obligation to delete it –which does not happen in the case of the right to be forgotten–[736]. Therefore, although they may appear to be the same, we are dealing with two different rights.

5.3.Access to information: right to know how the algorithm works

The new rights linked to automated decisional processes take on special relevance. These are a particular dimension of the principle of transparency of the algorithm. The decision-making process adopted by AI instruments is sometimes very difficult –or even impossible– to know, since they often act as a sort of black box, as we have already had occasion to explain. Linked to this is the "right to explanation", which consists of the right of the interested party to access information concerning the existence of an automated decision-making process and to obtain significant information on the logic used[737]. What happens, however, is that the mechanisms that work with neural networks do not lend themselves to directly providing comprehensible explanations of the way in which a certain conclusion has been reached. It is true that it is possible to arrive at the way in which the system has made the decision, i.e., it is possible to examine how the input has caused the activation of certain neurons and how the output has caused the activation of others[738]. However, this information is not explicit, it does not offer comprehensible justifications. At a first level, it is possible to identify the original algorithmic source code, the data entered into the system and the final result. As the number of nodes, the levels at which they are organized and the complexity of their connections increase, it becomes more difficult to know[739].

[735] *Ibd.,* pp. 288-289.
[736] *Ibd.,* p. 290.
[737] FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?...*, cit., p. 83.
[738] SARTOR, G. *L'Intelligenza artificiale e il Diritto...*, cit., p. 59.
[739] BLOUNT, K., "Using artificial intelligence to prevent crime...", cit. According to SARTOR, although the system acts as a sort of black box, it is possible to perform some critical analysis of the behaviour. Thus, it is possible to determine the predictors that have led to the result through, for example,

In the current context, the right of access to information or explanation is modulated, as the individual must be able to know and understand the reasons why a system has reached a certain result, translating mathematical models into understandable language, understanding the reasons why a system has reached a certain conclusion[740]. Otherwise, discriminatory situations may arise if the mechanism emits biased results. In the specific case of surveillance, the conclusion will be affected if the initial data with which the algorithm works were flawed. In this line, the officer's discretion to act in conjunction or in accordance with the predictions of the algorithm is further affected by the content of the data used by the AI. In BLOUNT's opinion, the citizen-police relationship changes with the use of algorithms, because the officer's discretion is no longer based on his own observations and knowledge, but on the judgments made by the mechanisms[741].

Other emerging rights are the right to disconnection and the right to autonomy in relation to the machine[742]. Although they are of a new type, all the aforementioned rights can be traced back to the traditional ones, and can thus be described as specific variants of those[743]. Thus, the general instruments of protection would serve a priori as a framework of protection.

IV. LIMITS TO FUNDAMENTAL RIGHTS: PROPORTIONALITY AND STRICT NECESSITY CRITERIA

The exercise of rights and freedoms is not absolute and can be limited as long as it is provided for in the law[744] and there is another legitimate interest at stake. In this case, it would consist of the state of maintaining public safety[745] through the prevention and control of crime. Art. 52 of the Charter allows for the limitation of rights in its first section, where it establishes the requirements to be considered for this purpose. Thus, any restriction must be provided for by law and respect the essential content of the rights. In addition, account must be taken of the principle of proportionality, according to which limitations may only be introduced where they are necessary and actually meet objectives of general interest recognized by the Union or the necessary protection of the rights and

sensitivity analysis, i.e., by systematically controlling which changes in the values of the predictors cause changes in the output. SARTOR, G. *L'Intelligenza artificiale e il Diritto...*, cit., p. 60.

[740] ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione...", cit. In the author's opinion, the programming of the algorithm becomes relevant in this case.

[741] BLOUNT, K., "Using artificial intelligence to prevent crime...", cit., p. 4.

[742] ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione...," cit., p. 151.

[743] Of the same opinion, *Ibd.* p. 152.

[744] CRAWSHAW, R. "Introduction to the seminar on human rights and the police: Human rights, the rule of law and policing", in *Human Rights and the Police. Seminar proceedings, Strasbourg 6-8 December, 1995*, Council of Europe Publishing, 1997, p. 13.

[745] PÉREZ TRENCH, N. "Los sistemas de reconocimiento facial...", cit., p. 64.

freedoms of others. The third paragraph of the same refers to the Convention, in the sense that when the rights provided for in the Charter correspond to those contained therein, their meaning and scope shall be identical.

On the contrary, the Convention does not contain any specific precept providing for the possible limitation of rights and freedoms, but rather the requirements for this are stipulated in each specific case. As far as we are concerned, those that are of interest to our study, namely, arts. 8 (respect for private and family life), 10 (freedom of expression), and 11 (freedom of assembly and association), also known as restricted rights[746], can be limited in the situations and under the conditions established in the second paragraph. All of them, in practically identical form, state that they may not be subject to restrictions beyond those provided for by law and are necessary measures in a democratic society to, among other purposes, guarantee national security, public safety, the defence of order and the prevention of crime or the protection of the rights and freedoms of others. Thus, what is established in this case coincides to a large extent with the content of art. 52.1 of the Charter.

In view of the above, we will address the principles of regulatory foresight, proportionality and strict necessity in a democratic society, which are closely linked to each other. Furthermore, as the FRs use biometric facial data to operate, the processing of which is subject to data protection regulations (and must also be subject to a strict test of necessity and proportionality)[747], in order not to repeat what has already been discussed, we refer the reader to the analysis made in the section corresponding to the right to the protection of personal data to learn about the requirements to which these systems are subject. However, without prejudice to the fact that at some point we will refer to this regulatory framework to complete the aspects that may be necessary.

1. Provided for in a specific law

As stated above, one of the requirements established in article 52.1 of the Charter and the second paragraph of articles 8, 10 and 11 of the Convention is the existence of a specific legal basis in the domestic law of the State. Otherwise, it will imply a violation of rights without the need to observe other aspects[748]. The notion of legal provision,

[746] CASADEVALL, J. *El Convenio Europeo de Derechos Humanos, el Tribunal de Estrasburgo y su jurisprudencia*, Tirant lo Blanch, Valencia, 2012, p. 169.

[747] However, we must bear in mind, as stated by the FRA, *Facial recognition technology...*, cit., p. 24, that the initial processing of biometric images and the consequent retention of the sample and comparison of the data with a list already interfere with the right to privacy and the protection of personal data. The processing of this type of data is a limit to the aforementioned rights, which is why it must be subject to a strict test of necessity and proportionality, including the legal basis for doing so and the legitimate aim pursued. This assessment must take into account the context and circumstances as well as the sensitivity of the data or the way in which they are used. This will be discussed in more detail in this section.

[748] ECHR, *Case Djavit An v. Turkey*, paras. 68, 69.

according to CASADEVALL, refers to the quality of the provision, which must be compatible with the pre-eminence of the law, as well as accessible and foreseeable[749] . Likewise, it must be sufficiently clear in its terms to provide the public with an adequate indication of the conditions and circumstances under which the authorities are empowered to adopt the measure restricting rights[750], i.e., foreseeable for the public. In our case, it refers to the collection of biometric facial data for use in the identification of individuals through the FRs inserted in CCTV and conventional video surveillance systems.

This also applies in cases where such a measure is used for secret surveillance in the police sphere. Thus, already in 1978, the ECHR *Case Klass and others v. Germany*, for the control of correspondence, considered that this was an exceptional and necessary situation in a democratic society, in order to maintain national security, the defence of order and the prevention of infractions, in this case, by the threat of terrorism. It admits the existence of normative provisions that grant powers of secret surveillance to the State, which also has a certain discretionary power to choose the modalities of surveillance, although it does not understand it to be of an exploratory or general type. In this case, even though there was an interference with the right to privacy, it was legitimate because it was expressly provided for in a law[751]. Thus, in para. 59, it states that the legislation under analysis in this particular case contained certain clauses aimed at limiting the effect of the surveillance measures to an unavoidable minimum and ensuring that the aforementioned limitations were carried out in full compliance with the law, which was the case. In this sense, there is a certain conciliation between, on the one hand, the imperatives of defending a democratic society and, on the other hand, safeguarding the rights of the population.

In order for the law to be adequate and the use of FRs to be lawful, the guarantees must be established in a concrete and specific manner. Thus, the same Court holds in the judgements *Case Shimolovos v. Russia* and *Case Vukota-Bojić v. Switzerland,* specifically in its paras. 68 that "the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data". They also propose a series of measures or safeguards to prevent abuses that may result from the lack of public scrutiny: the duty to specify the nature, purpose and duration of the measure, the reasons necessary to order them, the authorities competent to permit, carry out and supervise them, and the type of remedy provided by national law[752].

[749] CASADEVALL, J. *The European Convention on Human Rights...*, cit., p. 170.

[750] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 15.

[751] Interesting is para. 50, which states that whatever the surveillance system adopted, there must be adequate and sufficient safeguards against abuse. It goes on to point out that this assessment is relative in nature because it depends on all the circumstances surrounding the case.

[752] ECHR *Case Vukota-Bojić v. Switzerland* and *Case Shimolovos v. Russia*. In the same vein, ECHR *Case Uzun v. Germany*, para. 63.

Similarly but in other terms, the ECHR *Case Piechowicz v. Poland* at para. 212 states that the expression "in accordance with the law" does not only imply compliance with domestic law but also relates to the quality of the law[753]. In the specific case of biometric data in relation to this aspect, the concurring opinion of Judge Koskelo joined by Judge Felici in the ECHR *Case Catt v. The United Kingdom* is very interesting. In it, the judges state that special vigilance is needed when assessing the quality requirements of the law

At the state level also, the Ruling of the First Chamber of the German Federal Constitutional Court of February 16, 2023 (1 BvR 1547/19, 1 BvR 2634/20) establishes a series of criteria and guarantees to be observed in the specific case of automated data processing. It considers it to be legitimate and necessary in the field of crime prevention provided that it is done for the purpose of increasing the effectiveness of serious crime prevention in the context of evolving information technologies by obtaining indications of imminent serious crimes that would otherwise go unnoticed in the police database. It echoes that law enforcement authorities are currently faced with a constantly growing volume of data that is increasingly heterogeneous in terms of quality and format, which is why it understands that it would be very difficult for knowledge to be obtained manually (para. 52). As the use of automated systems is only permitted for the protection of particularly important legal interests (life, physical integrity or personal freedom), a sufficiently identifiable danger is required and the presupposition of use needs to be specified for the specific admissibility of the systems.

The Court indicates the minimums that the law must regulate and establishes the prohibition of self-learning systems. These minimums are: (a) the databases that can be included and the extent to which they can be automated; (b) limiting automated use to which only qualified police employees have access; (c) data obtained from home surveillance or online searches used in a data analysis or evaluation to prevent crimes from being committed; d) limitation of further use in specific investigations; e) regulation of technical and organizational precautions; f) information from mass data collection must be marked or separated in advance; g) legal reserve on the type and scope of data; h) restrictive specifications for the method of data used. In addition, limitations on time and scope of data and permitted processing methods must be observed.

Authorization must be obtained when the measure is intended to be implemented in individual cases in which the aim is to obtain clarification of the facts. With regard to technical and organizational safeguards, the principle of proportionality translates into requirements of transparency, individual legal protection and supervisory control. Due to the high standards required by the Court, the German laws under consideration were declared unconstitutional. Regarding the purpose that legitimizes the restriction of rights and, in particular, on the indications of the existence of a concrete danger, it understands that the facts must allow to conclude that the event is at least of a specific type and foreseeable in time and that certain persons whose identity is known at least enough for the adoption of the surveillance measure will be involved, to be used specifically against them and to be largely limited to them. In the case of the judgment it is said that the specific danger required was not given, the reason for the intervention was disproportionately broad compared to the seriousness of the intervention described. The reason for the intervention is not specified and the requirement of at least one specified danger is not met, only "expected crime" is mentioned, which is insufficient. In the Court's view, more detailed specifications are required in the form in which they have been described. Thus, it would need to be examined whether the individual data included in the analysis are adequate to contribute to the prevention of crime that may be imminent.

It limits the scope of the function creep, in the sense that further use of the data within the original purpose can only be considered by the same authority within the scope of an identical task and for the protection of the same legal interests that were at the basis of the data collection. Therefore, a restriction is placed on possible further use by specifying a "sufficiently specific" purpose beyond that which motivated the collection measure for other purposes. Each new use must be justified by an urgent or sufficiently specific danger.

In view of the above, COTINO HUESO considers that the decision is very demanding and rigorous, even excessively so, in setting standards of guarantees and legislative quality. COTINO HUESO, L. "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial...", cit., p. 16. However, in our opinion, although rigorous, it is necessary to establish the minimum standards that all legislation providing for the implementation of measures involving automated data processing must have.

[753] In the same vein, ECHR *Case Uzun v. Germany*, para. 60. The quality of the law is linked to the possibility that it is accessible to the person involved, who must also foresee its consequences and be compatible with the rule of law.

governing the processing by the police of personal data, including sensitive data, for the purpose of monitoring threats to public order. While the collection and further processing of such data are an indispensable part of the functions of LEAs, there are at the same time significant risks of abuse with regard to the exercise and protection of the rights and freedoms of the individuals whose data are processed. A sufficiently rigorous approach is therefore necessary when assessing the quality of the regulations. In particular, the degradation of respect for democratic norms and the rule of law, of which there is growing evidence in several States. The standards of the Convention need to be considered in the light of the dangers arising from such developments for the protection of fundamental rights and freedoms.

Not only that, but, as noted above, the requirement of foreseeability[754] must be observed, as opposed to any absolute discretionary power in order to protect the individual against arbitrariness[755]. In this sense, the ECHR *Case Uzun v. Germany*, para. 61, establishes that in the context of covert surveillance measures, the rule must be sufficiently clear in its terms to provide the public with an adequate indication of the conditions and circumstances under which the authorities are empowered to adopt such measures. Given the risk of abuse inherent in any secret surveillance system, any measure must be provided for in a law and be particularly precise, especially as the technology available for its use is becoming increasingly sophisticated[756]. The Court in the *Case of Centrum För Rättvisa v. Sweden*, develops what is to be considered foreseeability in this area. It states in para. 247 that it is not the same as in other settings, since in that setting it cannot mean that individuals must foresee when the authorities will resort to such measures to adapt their conduct. However, he states that when a state power is exercised in secret, the risks of arbitrariness are obvious. For this reason, it reiterates that clear and detailed rules on the secret surveillance measures adopted are essential in order to provide the public with an adequate indication of the circumstances and conditions under which the authorities are empowered to carry out such actions. Notwithstanding the above, this criterion does not require States to list exhaustively the offenses that may justify the implementation of the measure, being sufficient the establishment of adequate provisions on the nature of the offenses in question[757].

[754] See also paras. 61 and 62 of the ECHR *Case Szabó and Vissy v. Hungary*.

[755] CASADEVALL, J. *The European Convention on Human Rights*, cit.

[756] In this case, the Court examines the interference with the right to respect for private life by the implementation of a GPS surveillance system. It considers that interference with communications is supported by German law, which is why there are a number of safeguards aimed at preventing abuse (see paras. 64 and 65). Specifically for this case, it considers that the measures provided for in the national legislation were sufficient to prevent abuse, including the principle of proportionality (para. 73).

[757] O'LEARY, S., "La surveillance de masse et la Convention Européenne des Droits de l'Homme...", cit., pp. 272-273. The author notes that the CJEU criticizes that the Union and national legislative measures it examined were not limited to a conservation of the data retained and the time period or geographical area, including the circle of individuals likely to be involved in a serious infringement. For the ECHR, it is the precision of the law that counts when it comes to specifying the categories of individuals who may be subject to surveillance. This imposes the requirement to strike a balance between precision, effectiveness and preventive capacity.

Therefore, whenever there is a desire to limit the exercise of any right, it will be necessary to adopt measures and foresee certain conditions to ensure it to the maximum extent possible, and these should be reflected in the domestic legislation of the State in question. In our case, they should specify the types of crimes in which the FRs would be applicable, the appropriate threshold of seriousness of the same, in order to exclude from their scope of intervention common crime[758]. In this regard, the CJEU *Digital Rights* Judgement repeatedly establishes that serious crimes constitute the criterion for verifying the purpose and proportionality of the interference with the fundamental rights to privacy, protection of personal data and freedom of assembly and association[759]. Thus, extrapolating the above to the implementation of FRs, such mechanisms would only be appropriate for the prosecution of serious crime, and all the above guarantees and measures must be clearly and specifically reflected. Otherwise, i.e., when the national legislation is not sufficiently exhaustive and does not expressly provide for the above requirements and measures and, even so, it is decided to implement such systems, this would be an intolerable violation of the rights and freedoms of citizens.

It is not only in the area of rights protection legislation that the requirement of legal foresight is established, since art. 10 a) LED includes the need for authorization by the law of the Union or of the Member State in question as one of the limits to the prohibition of the processing of special categories of data. Recital 33 of the same body of law states, in line with the ECHR and the CJEU (as set out above), that the legal provision must be clear and precise and its application foreseeable for those subject to it[760].

ECHR case law has established a series of minimum requirements in the case of interception of communications that must be contained in the law to prevent abuses of power and that can be extrapolated, *mutatis mutandi*, to the FRs: 1) nature of the offenses; 2) definition of the individuals subject to the measure; 3) limit on the duration; 4) procedure to be followed in examining, using and storing the data obtained; 5) precautions to be observed when the data are communicated to third parties; and 6) circumstances under which the data must be deleted or destroyed[761].

[758] See, in this regard, CJEU *Case C-817/19*, paras. 150 and 151.

[759] CJEU (Grand Chamber) Joined Cases C-293/12 and C-594/12. *Digital Rights Ireland Ltd*, 8 April 2014. ECLI:EU:C:2014:238. This pronouncement was followed some time later by CJEU (Grand Chamber) Case C-207/16, 2 October 2018. ECLI:EU:C:2018:788.

[760] Such regulations should at least contain the purposes of the processing, the personal data to be processed, the purpose, the procedures for maintaining the integrity and confidentiality of the personal data and the processes to be followed for their destruction. It considers that this provides sufficient safeguards against the risks of abuse and arbitrariness.

[761] See, i.e., ECHR *Case Centrum För Rättvisa v. Sweden*, para. 249.

This same pronouncement, in paragraphs 250 and 251, establishes the need for supervision and review of the measure in three phases: when it is ordered, during deployment and once it has concluded. Due to the secret nature of the measure, in the first two phases the review is carried out without the knowledge of the affected party. Therefore, the procedures established must offer adequate guarantees to protect their rights, through judicial supervision in order to ensure independence, impartiality and correct procedure. Already in the third phase, once the surveillance measure has ended, the question of notification is relevant to assess the effectiveness of the remedies brought before the courts and, therefore, the existence of effective safeguards against abuse of the surveillance power. If the interested party is not informed, the

The AIA in recital 34, for the cases in which it allows the use of RBIS in real time, in line with the above limits, establishes that, in order for such systems to be used responsibly and proportionately, they can only be deployed once a fundamental rights impact assessment has been carried out and if the mechanism has been registered in a database of those established in the Regulation. In addition, the reference database must be appropriate for each of the situations. The elements relating to the nature of the same, the consequences of their use on the rights and freedoms at stake, as well as the guarantees and conditions to be observed must also be taken into account. It goes on to indicate that limits must be established in relation to persons, time period and geographical and personal scope. To this is added the need for prior authorization by a judicial or administrative authority independent of the State[762], except in exceptional circumstances motivated by urgency, in which case, likewise, the appropriate safeguards must be observed and limited to the minimum necessary (recital 35). The specific situations are specified in art. 5(h) of the AIA, namely, targeted search for victims and missing persons, prevention of threats to life or safety or threat of terrorist attack, and location or identification of individuals suspected of having committed a serious crime, to which is added the obligation to specify the geographical area and time limit.

Therefore, if the LEAs follow all of the above, by virtue of the AIA and, as provided for in the national regulations, they would be making lawful use of the FRs, at least as far as compliance with the regulatory provision is concerned. A different matter –we reiterate– occurs with those that act in deferral because, as we have repeatedly indicated throughout this research, the way in which they are to be deployed is not so exhaustively and limited, when the damage to rights and freedoms may be even greater in the latter case.

As the AIA establishes the way to develop and implement the RBIS and the consequent processing of personal data, the question immediately arises as to whether it would serve as the legal basis required both in the previous article and in article 8.2 LED for the processing of personal data to be considered lawful[763]. We must immediately answer in the negative, since recital 38 of the AIA states that it "is not intended to provide the legal basis for the processing of personal data" as established in the two aforementioned precepts. This means that Member States wishing to use the exceptions offered by art. 5 h) AIA do not have to incorporate the clause relating to "authorized by Union law". They are therefore able to use these exceptions if they adopt clear and

scope for recourse is limited. This requirement is therefore necessary for the legality of the measure to be challenged retroactively.

[762] The ECHR considers this requirement - in the case of mass interception of communications - as an important safeguard against arbitrariness. *Case Centrum För Rättvisa v. Sweden*, para. 265. It continues in para. 266 by stating that the independent entity in charge of the authorization must be informed of the purpose of the interception and of the carriers or means of communication that may be intercepted, which will allow this body to assess the necessity and proportionality of the operation.

[763] This provision stipulates that the law of the Member State must at least indicate the purposes of the processing, the personal data to be processed and the purposes for which they are to be processed.

detailed rules, which is why the regulatory basis will have to be developed at the State level.

Likewise, it is up to the countries to decide whether and how to introduce these systems, as stated in recital 37 of the AIA. Therefore, the debate on the opportunity to prohibit the use of RBIS by LEAs in public accessible places has been nationalized, taking into consideration the provisions of the AIA. Problems arise from this due to the fact that each country is called upon to create its own regulatory system on these mechanisms, from which derives the risk of fragmentation in Europe, extending also to questions regarding the proportionality and necessity of the measure. Added to this is the question of how to achieve consistency and coherence in view of the terms on how to interpret the legal requirements imposed by the AIA[764].

In the case of deferred systems, recital 39 of the latter refers to the personal data protection regulations and must comply with their content. Therefore, a solid regulatory basis is required, detailing all aspects related to their deployment and implementation. The AIA establishes the requirements and measures to be observed by high-risk systems (among which are those)[765], so that in principle it could act as such a regulatory basis. However, due to the insidious nature of the technique and, for its proper implementation, we consider that it should be expressly provided for in an *ad hoc* regulation, specifying the cases in which it can be used, since it is not specified in the AIA, nor are the specific guarantees to which it must be subject. Recital 95 only limits itself to pointing out (we reiterate) that its deployment must be proportionate and legitimate, to the extent strictly necessary, but what is strictly necessary in this case? The aforementioned recital alludes that this is linked to the limitation of the persons to be detected, the location and the temporal scope, for which a limited set of video recording data that have been lawfully obtained must be used. In our opinion, this provision is excessively broad and may lead to a situation of mass surveillance, which is already echoed in the final part of the aforementioned recital. For this reason, it would be necessary, as we have said, for a regulation to expressly provide for all the guarantees, requirements and limits of its use.

On the need for regulatory provision in the specific case of FRs, in the *R Bridges v CCSWP and SSHD* judgement (cited above), the Court of Appeal of England and Wales found that, although the use of the systems was proportionate, there were no clear

[764] Of this opinion, CHRISTAKIS, T. BECUYWE, M. & AI-REGULATION TEAM. *Facial Recognition in the Draft European AI Regulation...*", cit., pp. 8-9.

[765] Without wishing to be exhaustive, the most important measures are described below. Thus, art. 9 develops how the risk management system should be; art. 10 is devoted to data and data governance, where special consideration is given to data quality, relevance and representativeness, in order to eliminate biases. Likewise, measures are foreseen to ensure security; art. 13 refers to transparency and the communication of information to those responsible for the deployment, which will include instructions for use with different information; art. 14 establishes the requirement of human supervision to ensure effective monitoring of the mechanism by natural persons during the period of use, in order to prevent or reduce the risks derived from it, which will be offered to the person responsible for the deployment so that they are aware of all the related aspects. Finally, art. 15 develops the requirements of accuracy, robustness and cybersecurity to be observed throughout the life cycle of the system.

guidelines as to where and when it could be applied. For that reason, this requirement is not met and does not comply with art. 8.2 of the Convention.

2. Proportionality test

The second of the criteria under study is the judgment of proportionality, which acts as a guiding principle to determine the limitations of rights[766]. By virtue of this, in the existence of a right that may collide with another, it must be verified whether the benefit derived from the protection of the former outweighs the harm that the restriction of the latter would entail[767]. This requirement is made up of three dimensions that must be observed:

a) Adequacy or suitability for the intended purpose[768]. This involves assessing whether a measure is adequate to achieve the objectives it is intended to achieve. This assessment includes the study of the importance of the purpose and the rational connection between the measure and that specific purpose[769]. The CJEU in *La Quadrature du net and others,* para. 164, states that the purposes on which the appropriateness of the measure adopted is based must be specified in a rule. In this case, it rules on the interference of the retention of personal data with arts. 7 and 8 of the Charter, which is only justified in the case of serious crimes and the protection of national security. Furthermore, in order to ensure that the measure is limited to what is strictly necessary, it lays down a number of conditions. Adequacy is therefore closely linked to the normative provision already addressed in the previous section.
   This criterion does not attempt to determine whether the costs outweigh the benefits, as this is a matter for the next two judgments[770].
b) Necessity, i.e., that the measure is essential to achieve the proposed objective and that there is no other less intense measure to achieve it. This test considers whether the restrictive measure is effective, i.e., essential to achieve the intended purpose and whether it is the least intrusive to the rights at stake.
   It is a matter of verifying the existence of alternative measures that are less harmful to the fundamental right in question and, among these measures, the

[766] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 520.

[767] PÉREZ TRENCH, N. "Los sistemas de reconocimiento facial...", cit., p. 66.

[768] This means that any measure disproportionate to its object is prohibited, which requires avoiding exaggeration when adopting restrictions on rights. Thus, what is disproportionate goes beyond what is necessary or proportionate. Para. 14 of the Dissenting opinion of Judge Serghides in the ECHR *Case S.J.P and E.S. v. Sweden.*

[769] PLACCO, A.V. "La protection des données à caractère personnelle dans le cadre de la jurisprudence de la Cour de Justice de l'Union Euorpéenne...", cit., p. 35.

[770] MOBILIO, G. "Your face is not new to me...", cit., p. 10.

degree of effectiveness in relation to the end pursued. In the absence of less harmful means, the one under consideration may be adopted[771].

c) Proportionality in the strict sense. The latter consists of assessing whether the limitation does not impose an excessive burden on the right holder. Thus, it is a comparison aimed at finding the balance between the costs (interference with rights) and the benefits (importance of the objective to be achieved in a given context). It is a matter of ensuring that the measure is not disproportionate and intolerable, so that there must be a fair balance between the measure adopted and the limited right[772].

   Thus, it can be said that it will be proportional if the restriction favours the public interest more than the sacrifice of the rights[773], from which it follows that the limitation of these must be done in the way that is strictly necessary to ensure the protection of the interests for which it is limited, with the benefits outweighing the harm[774]. The assessment of proportionality is always carried out *ex ante* in the legislation that contains it, but the test that is carried out at this point aims to determine *in concreto* the objective pursued and the way in which fundamental rights are affected in imagined scenarios where the measures offered by the law would be applied[775].

Let us now look at how it applies in specific cases. In the ECHR *Case Yefimov and youth human rights group v. Russia*, an individual was suspected of extremist crime and his name was included in a list of suspected terrorists, which in the case of this country is provided for by law, thus being understood to be a necessary action. What happens in this case is that such measures are implemented with little or no guarantees because they are automatic and are not subject to judicial control or review. Thus, the investigator is granted legal authority and full discretion to interfere with the right (in this particular case, to freedom of association). An unconditional restriction of its exercise is an extremely severe measure even in the case of a convicted person, and should therefore be justified by serious and compelling reasons; but even more so in the case of mere suspects, since they still benefit from the presumption of innocence (see paras. 60 and 61). For its part, in para. 62, the Court reiterates that the principle of proportionality must be observed in order to limit any fundamental right, which requires that there be a link between the

[771] PLACCO, A.V. "La protection des données à caractère personal dans le cadre de la jurisprudence de la Cour de Justice de l'Union Euorpéenne...," cit., p. 36.

[772] *Ibd.,* p. 37.

[773] In said sense, see SCC Ruling, 76/2019, 22 May 2019, [RTC 2019776].

[774] PÉREZ TRENCH, N. "Los sistemas de reconocimiento facial...", cit., p. 66.

Judge Serghides, in his dissenting opinion in the ECHR *Case S.J.P and E.S. v. Sweden*, differentiates between the latter criterion and the fair balancing test between the limiting measure and the right. The former refers to the balance between the means used and the end pursued, while the latter refers to the balance between a public interest and a private interest, or between several private interests. He considers that the proportionality test is not an independent balancing exercise between two variables, but is part of a broader balancing exercise. Thus, the right that is disturbed by the measure and the intensity of the limitation must be taken into account. In addition, the existence of any other measure or alternatives that are less intrusive or injurious in relation to the affected right must be considered.

[775] MOBILIO, G. "Your face is not new to me...", cit., p. 11.

application of the measure and the conduct and circumstances of the specific individual. Thus, the authorities are obliged to choose the means that cause the least possible harm to the rights at stake. What happens here is that Russian law does not require the assessment of proportionality. As a result, courts examining a complaint about the inclusion of an individual's name on the aforementioned list only have to make sure that it is based on a proper procedural document, prepared by an investigator. They are therefore not obliged to consider the evidence on which the decision is based or to assess the justification for declaring someone a suspect, taking into consideration the rules of the Convention and the presumption of innocence (para. 63). The Court concludes that the provisions of the Russian legislation that make the exercise of the fundamental right to freedom of association dependent on the investigator's decision to declare a subject as a suspect of a terrorist offense does not meet the criterion of the quality of the law either, since it grants unlimited discretion to the investigating authorities and does not provide protection against abuse, which is why it is not a proportionate measure.

With regard to secret surveillance, we refer to the ECHR *Case Centrum För Rättvisa v. Sweden*, which stems from the provision in Swedish national legislation of a system of secret surveillance potentially affecting the communication of all persons via telephone or Internet. The Court noted that the surveillance system was clearly provided for in the national legislation and justified on security grounds. It went on to state that, given the current threats of global terrorism and border-crossing crimes as well as the increasing sophistication of communication technologies, Sweden has broad discretion in deciding whether to develop a measure of mass surveillance of communications. The guarantees and safeguards with respect to the right to privacy were expressly contained in the law in the terms set out in the previous section. For all these reasons, it is concluded that the measure is proportional to the objective pursued (paras. 178-181). The Court further notes in para. 236 that States in this context have a legitimate need for secrecy, which means that little or no information about the operation will be made public.

In the above case, it is understood that the secret surveillance measure, consisting of the interception of communications, is proportionate, as in the *case Big Brother Watch and others v. The United Kingdom*, where the ECHR found no violation of the Convention because the conditions necessary to consider the limitation of rights legitimate were met, since this country had a legal basis, the interference pursued legitimate purposes and the positive law specifies the procedure for requesting the interception of communications and transmission of the material resulting from this practice. This pronouncement was not unanimously accepted and, Judge Pinto de Albuquerque, in his preliminary conclusion (para. 58), argues that the potential increase in surveillance activity in the last decade and the public outcry it has unleashed, justifies a stricter supervision of the activities of intelligence agencies, aimed at preserving democracy and upholding the rule of law. Not the opposite. When the risk of state abuse increases, the safeguards of the Convention and the corresponding guarantees of domestic law must also increase, not decrease. For that reason, the Court's standards should also be higher but this is not the case in this

judgement, where the Judge believes that the Court has succumbed to general mass interception, dangerously accepting that if it is useful, it must be allowed. He goes on to rightly point out that utility is not the same as necessity and proportionality. For that reason, he concludes by stating that one must be more vigilant in protecting liberty when the aims of the State are not laudable.

On the contrary, the ECHR *Case Breyer v. Germany* ruling on the storage of data by telecommunications service providers. A 2004 amendment to the German law regulating them allowed the collection and storage of all customer data, even that which was not necessary for billing or other contractual reasons (prepaid SIM cards for cell phones). Prior to this reform, providers were only entitled to collect and store data necessary for their contractual relationship. The alleged purposes for the change were the prevention and prosecution of crimes or regulatory violations and the performance of intelligence functions. The Court states in para. 88 that the fight against crime, especially organized crime and terrorism, is one of the challenges facing European society today, making the maintenance of public safety and the protection of citizens a social necessity. It also recognizes that modern means of telecommunications and changes in communication behaviour require the investigative tools of national security and law enforcement agencies to adapt. In para. 90, for its part, it supports the indicated measure, while recognizing that pre-registration of cell phone subscribers greatly simplifies and accelerates the investigation and can contribute to effective law enforcement and the prevention of disorder or crime. It also reiterates that, in a national security context, the authorities enjoy a certain margin of discretion in choosing the means to achieve a legitimate objective and notes that there is no consensus among Member States as regards the retention of prepaid SIM card customer information. Against this background, and taking into account this margin of appreciation, the Court accepts that the obligation to store customer information under the Telecommunications Act was, in general, an appropriate response to changes in communications behaviour and telecommunications media. Despite this, it is questioned whether the interference is proportionate. After analysing all aspects of the regulation, especially the guarantees and requirements established to protect the exercise of the right provided for in art. 8 of the Convention, it maintains in para. 109 that it was a proportionate and necessary measure in a democratic society, and therefore it understands that the content of the aforementioned precept was not violated.

In view of what has been said so far, we can affirm without difficulty that the judgment of proportionality is difficult to measure. This is echoed by GABA/ESTREMADURA when they state that it is governed by the balancing test of the interests at stake, which depends on the interpretation of the competent authority to make the assessment[776], which will have to take into account the particular circumstances of the

[776] GABA, J.P.M. & ESTREMADURA, J.J.M. "Data protection of biometric data and genetic data", *Ateneo Law Journal*, vol. 64, 2019, p. 972. The authors refer more specifically to the GDPR and the

case and the level of violation of the right at stake by the application of the measure[777]. Thus, for example, the ECHR *Case Internationale Humanitäre Hilfsorganisation e.V. v. Germany*, on interference with freedom of association, the Court holds that there is a margin of appreciation by the Court given the specific circumstances of the case and, taking into account the exhaustive balancing exercise carried out by the national courts and the important interests involved (given that the association appeared to finance terrorist activities), the national authorities had relevant and sufficient reasons and did not exceed the margin of appreciation. It concludes that the interference with the data subject's right of association was proportionate to the legitimate interests pursued.

All of the above refers to the proportionality test in a general sense or as applied to the surveillance scenario, but what about the use of biometric data and more specifically the operation of FRs in this context for the purpose of crime prevention. As can be seen from the aforementioned ECHR *Case S. and Marper v. The United Kingdom*, the Court held in para. 125 that the powers of indiscriminate retention of biometric data of suspects does not strike a fair balance between public and private interests and, as such, the State exceeded any acceptable margin of appreciation. Thus, the retention of such data constitutes a disproportionate interference with the right to privacy and cannot be regarded as necessary in a democratic society[778]. For this reason, the State would have exceeded any acceptable margin of appreciation[779].

More specifically, with regard to FRs, it should be pointed out that they should only be chosen if the end pursued cannot be achieved with other measures that are less

processing of biometric data in the private sector but it is perfectly extrapolable to the maintenance of the law.

[777] In the case, for example, of the measure of preventive detention and its reasonable period, the ECHR *Case Dervishi v. Croatia*, in para. 130, holds that it cannot be determined in the abstract, but must be assessed in each case according to the specific characteristics. Thus, continued detention can be justified only if there are specific indications of a genuine public interest requirement that, notwithstanding the presumption of innocence, prevails over individual liberty.

[778] On the principle of proportionality and the processing of biometric data in particular, see extensively ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed...", cit. pp. 9-10. The authors argue that this principle of proportionality has virtuality throughout the entire life cycle of information processing, from the design and selection of techniques to the disposal of the data collected. The aim is to prohibit behaviour that would result in indiscriminate, irrelevant or excessive processing. The proportionate collection of this type of data is one of the major challenges relating to the requirement of proportionality. It is inherent in the procedure of processing biometric data that the data subject is only identified and the intended purpose is achieved at the end of the process, after the raw and sample data are collected, the biometric data are enrolled to extract relevant measurements, the biometric template is created, which can then be stored and compared to make the final determination as to whether the compared templates match.

However, the authors understand that this makes proportional data processing difficult because a database contains very diverse information with different degrees of need or usefulness for the research, when not all should be processed indiscriminately. Thus, they propose that, to solve this problem, some safeguards can be adopted such as data relevance, quality and adequacy: a) explainability so that the human operator can understand how the system determines the relevance of the sources and data it records; b) investigation by a human to ensure the relevance and adequacy of the sources and data; and c) homogeneity, so that the data are derived from similar and predictable sources where the quality, accuracy and reliability of the source can be documented and scaled.

[779] O'LEARY, S., "La surveillance de masse et la Convention Européenne des Droits de l'Homme...", cit., pp. 257-258.

intrusive to the fundamental rights and freedoms of individuals, as there must be a balance between the two[780]. In this sense, in relation to the costs, it is necessary to take into account the context in which the surveillance takes place (public spaces frequented by an indefinite number of people), the purpose, which in principle should be restricted to a specific type of individuals, the level of intrusiveness (very high in the case of identification) and the fundamental rights that would be affected; while the benefits take into account the needs and importance of the objectives pursued, being linked in this case to border security or surveillance in uncontrolled spaces; and the seriousness of the crime pursued, since the prevention of terrorism is not the same as theft by pickpockets[781].

In line with what has just been indicated, in our view, the objective of maintaining security and preventing crime, including serious crime, can be guaranteed with conventional video surveillance systems without the need for them to incorporate the FR technique, since the former, although it raises certain controversies, is a less restrictive measure of the rights and freedoms of citizens[782]. In addition, as stated by RAPOSO, sometimes they do not provide real benefits to society, since the effectiveness of the mechanism does not depend on the number of persons arrested but on whether they are arrested for committing serious crimes, since if they have not yet committed any serious criminal offense and have been identified by the system and arrested, there is no real benefit[783], to which we add the high percentage of false positives of the technique.

In our opinion, even if the FRs are included in a regulation, we are dealing with a technique with very high levels of harm and, as will be seen in the following chapter, the exact benefits they bring in terms of security are not known, since it is a very difficult question to assess. The fact that a measure of such characteristics, i.e., restrictive of rights and freedoms, involving secret and constant surveillance of citizens, is provided for in a law, is not sufficient justification for its implementation. The specific circumstances must be assessed on a case-by-case basis, and high standards of protection must be established when evaluating the proportionality of its adoption, scrupulously analysing compliance with the three criteria that make up this criterion. Following what Judge Pinto de Albuquerque has already stated, the fact that an action is useful for the State does not imply that it is proportional and necessary. Thus, we should not relegate the exercise of

[780] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 521.

[781] MOBILIO, G. "Your face is not new to me...", cit., p. 11.

[782] Although it also raises some controversies in relation to them, they do not represent an interference of the same level as the FRs. On the problems of video surveillance systems in the public sphere, see, in more detail, GIL MEMBRADO, C. *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*. Wolters Reuters, Madrid, 2019; & HOLLIS, M.E. "Security or surveillance: Examination of CCTV camera usage in the 21st Century", *Criminology and Public Policy*, vol. 18, nº. 1, 2019, pp. 131-134.

Other less rights-restrictive measures that can be used in lieu of FRs include additional staffing, increased police frequency, or improved lighting conditions in public spaces. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0...*, cit., p. 17.

[783] RAPOSO, V.L. "The use of facial recognition technology by law enforcement in Europe...", cit., p. 521. However, the author maintains that there would be a benefit in serious crimes such as terrorism or child pornography.

our rights and freedoms as citizens of a democratic society for the sake of a supposedly greater security.

3. Strict necessity in a democratic society

As has been shown in the previous section, most of the decisions analysed tend to refer, together with proportionality, to the necessity of the measure in a democratic society, linking both as guiding criteria on the appropriateness of the restriction of rights and freedoms.

The expression "necessary in a democratic society", as stated in the ECHR *Case Piechowicz v. Poland* at para. 212, means that the interference with the law must correspond to a pressing social need and, in particular, must be proportionate to the legitimate aim pursued[784]. In assessing whether an interference is necessary, as with the previous criterion, account must be taken of the margin of appreciation left to the State authorities in deciding how best to achieve the legitimate aim of protecting security[785], with the State also having the burden of proving the existence of such a pressing social need underlying the interference.

In the event that national legislation provides for secret surveillance, the legality of the specific measure to be implemented is linked to the evaluation of this test and its requirements. Thus, the "quality of the norm" implies that the national law must not only be accessible and predictable in its application, but must also ensure that the measures adopted are applied only when "necessary in a democratic society", in particular by providing safeguards and guarantees against abuse[786]. These will depend on the circumstances of the case (nature, purpose, duration and possible measures, the grounds for ordering them, the authorities competent to authorize, develop and supervise them, and the type of remedy provided by national law), with the Court being competent to

[784] In the same sense, *Case Uzun v. Germany*, para. 78. Examining the case in question, it concludes that the GPS surveillance measure was not ordered from the beginning, as the investigators initially used other measures that interfered less with the right to privacy but proved ineffective, which is why it was decided to develop it. In para. 75, the Court considers that the observation of the interested party's conduct had been very extensive and there had been a serious interference in his private life, so that GPS surveillance required more convincing reasons to justify it. This surveillance took place over a relatively short period of time, affecting him only on weekends and when he was traveling by car. Therefore, it is concluded that there was not total and comprehensive surveillance. Moreover, the objective was to prosecute very serious crimes, more specifically, several assassination attempts on politicians and public officials with bombings. For all these reasons, the Court holds that the surveillance carried out with this measure in the specific case was proportionate and, therefore, "necessary in a democratic society".

[785] In this case, as is clear from the ECHR *Case Centrum För Rättvisa v. Sweden*, para. 261, in the interception of communications, which can be extrapolated to the FRs, there is a risk of abuse that may adversely affect the right to privacy. The Convention prohibits this type of interception to protect national security and other essential interests against external threats, but it is dangerous to leave a wide margin of appreciation to the States when deciding on the measure, so it should be more restricted and have specific safeguards.

[786] ECHR *Case Centrum För Rättvisa v. Sweden*, para. 248.

determine whether the procedures for supervising the ordering and implementation of the measures limit the interference of those considered necessary[787].

The Court, in para. 91 of the *Case SH and others v. Austria* Judgement, argues that, to meet this requirement, it must be observed whether the reasons to justify the measure are relevant and sufficient for the purposes of the rights at stake. For this reason, the assessment must be made in the specific case. Thus, the *Szabó and Vissy v. Hungary* Judgment holds in para. 73 that such a measure must be strictly necessary for the safeguarding of democratic institutions and will only be appropriate if it is the only (or, in the words of the Court, strictly necessary) measure by which the end pursued can be achieved. Otherwise, it is likely to facilitate abuse by those who have the power to implement it. To this he adds that the absence of prior judicial authorization favours the discretion of the authorities. One of the issues that arise when assessing the authorization of the measure and its application is the absence of judicial control, given that, although the security services have to indicate in their requests the need for the measure, the procedure does not guarantee that an assessment of strict necessity has been carried out[788].

The EDPB also rules on the criterion of "strictly necessary" with regard to the processing of personal data carried out by LEAs on FRs. According to the agency, the measure may be developed when the restriction it entails on rights and freedoms is limited to what is considered strictly necessary. It further argues that the term "strictly" obliges the legislator to observe even more restrictive conditions than mere necessity, thereby restricting the margin of appreciation to an absolute minimum. Furthermore, it links it to the requirement to rely on objective criteria to define the circumstances and conditions under which the prosecution may be carried out, excluding any other of a general or systematic nature[789].

However, the essential question we ask ourselves at this point is, does the FRs constitute a proportional and necessary measure in a democratic society? We have already indicated above that, in an attempt to reduce the use of such mechanisms to what is strictly necessary, situations are limited in the case of mechanisms acting in real time in the first paragraph of letter h) of art. 5 AIA, but the impact on fundamental rights and freedoms in view of the principle of proportionality[790] and the characteristics of those must also be

[787] *Ibd.*, para. 253.

[788] ECHR *Case Szabó and Vissy v. Hungary*, para. 75. The Court goes on to state in para. 77 that the political nature of authorization and supervision increases the risk of abusive measures.

[789] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement...*, cit., p. 21.

[790] MILOSSI, M. "Remote biometric identification systems and ethical challenges...", cit., p. 5. As SCHEPISI argues, in the three cases in which the use of RBIS in real time is foreseen, the right to privacy and protection of personal data (also dignity and the others analyzed throughout this Chapter), may yield to security threats. SCHEPISI, C. "Diritti fondamentali, principi democratici e *rule of law*...", cit. However, he argues that if the system operates a posteriori, priority is being given to the fundamental right to privacy and the protection of personal data (hence the legal basis of Art. 16 TFEU as well as Art. 114 TFEU) over the right to security that could be guaranteed by a general mass surveillance activity for the fight against crime. In our opinion, the above approach is inadequate since the deferred mechanisms also entail an intolerable interference with fundamental rights that are subordinated to security. It goes on to state on p.

taken into account when assessing this requirement of strict necessity. Therefore, in the following section, we will deal with these exceptions.

4. Specific cases in which facial recognition system can be used according to the article 5.h) AIA

Firstly, the selective search for missing persons and victims of certain crimes such as kidnapping, human trafficking or sexual exploitation. In this specific situation (whose incidence is very high[791]) in our opinion, the FRs would be beneficial and would be an appropriate measure for the intended purpose due to issues such as the difficulty in many cases to find missing individuals for the reasons mentioned above, as well as aspects of immediacy and speed, in the sense that the identification must be done quickly to avoid violating the legal rights that are threatened by the crimes indicated in the precept; or simply to return these people to their places of origin. In this area, technology is proving to be a powerful tool for LEAs due to its ability to process large amounts of data from different sources such as social networks or CCTV in a very short time. In addition, its inclusion in video surveillance systems makes it possible to identify individuals in real time. Thus, the efficiency and accuracy of the systems are its two main benefits[792]. However, despite the positive aspects of the technique, we should not forget its negative issues.

Some mechanisms have already been developed for this purpose. Thus, one method for the identification of missing persons still alive is that proposed by RAJ et al., which allows the comparison of the facial characteristics of unidentified persons with a database of missing persons, using high-resolution images and advanced algorithms[793]. At the international level, INTERPOL uses this tool for various purposes, including the identification of persons of interest or missing persons[794]. Other institutions are also working on the application of FRs in the identification of missing persons. For example, the Red Cross is in the process of creating software to help locate missing migrants. This work is carried out for humanitarian reasons and will facilitate the matching of remains found with images provided by relatives[795]. Nowadays, migratory movements are very

230 that the State may be responsible for the direct application by the public authorities themselves of algorithmic systems that are not respectful of Charter rights or do not monitor their respect and prevent inappropriate use.

[791] In the case of Spain, see the *Annual Report. Missing persons during the year 2023* of the Ministry of the Interior, pp. 32-35.

[792] RAJ, P. et al. "Facial recognition system for identification of missing person," *Kalpa Publications in Computing*, vol. 19, 2024, pp. 323.

[793] *Ibd.*, pp. 322-332.

[794] INTERPOL, *Facial recognition*. Electronic resource obtained via the World Wide Web: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial, [retrieved on 29 August, 2024].

[795] RED CROSS, *Red Cross works on facial recognition software to help locate missing migrants*, 28 August 2024. Electronic resource obtained via the World Wide Web: https://www2.cruzroja.es/-/cruz-

high and, during the crossings, individuals go missing very often. For this reason, the implementation of an automated system to recognize and identify these people is very useful, speeding up the work of the organization. At the Spanish national level, the SOSDesaparecidos Association will also use the FRs. It is based on a volunteer action that aims to get citizens to collaborate by sending photographs of missing persons to the association, which will add them to a "Google Photos album" created *ad hoc* for this purpose. Once the image is received, it is sent immediately and privately to the LEAs and other international entities with which it collaborates.

Finally, another instrument that, from our point of view, is very interesting in the identification of deceased individuals, is the one developed between the University of Granada (Spain) and the Polish universities of Kraków and Wroclaw. Through it, it is possible to recognize a missing individual –in this case, deceased– through his teeth, comparing them with a photograph or video in which he appears smiling. This material may have been obtained either by family members or by downloading it from their social networks[796].

In the case of a specific, significant and imminent threat to the life or physical safety of persons, or when the threat is real and present or real and foreseeable terrorist attack, the FRs can be used. The aforementioned exception is not exclusive to these mechanisms, but also extends to other mass surveillance measures such as the interception of electronic communications, as was made clear by the CJEU in the *Case La Quadrature du Net (*paras. 136-138), where the Court understood that the State had the ability to derogate from the obligation to ensure the confidentiality of the data from the same. In this regard, it recognized that the importance of preserving national security extends to the fight against serious crime and may justify a superior interference with fundamental rights. It also accepts the use of algorithms to process the large volume of data derived from such data. The assessment of a situation as a serious threat is controversial, since it does not specify what is meant by it and, as we had occasion to

roja-trabaja-en-un-software-de-reconocimiento-facial-que-ayude-a-localizar-migrantes-desaparecidos, [retrieved 29 August 2024].

[796] When other biometrics cannot be used because they have deteriorated, teeth are very useful in identification work because they are one of the elements, along with bones, that remain unalterable and unique to each individual. MAZUR, M. et al. "Smile photograph analysis and its connection with focal length as one of identification methods in forensic anthropology and odontology", *Forensic Science International*, vol. 335, 2022, pp. 1-9.

Another interesting tool in this regard was also designed at the University of Granada in collaboration with the University of A Coruña (Spain). In this case, the aim is to superimpose the skull of a deceased person with *ante-mortem* images in a process of craniofacial superimposition. The objective is to identify human remains. To learn more about this instrument, see MARTÍNEZ-MORENO, P. et al. "Evidence evaluation in craniofacial superposition using likelihood ratios", *Information Fusion*, vol. 111, 2024, pp. 1-11. Although it is used in the case of individuals once they have died, we believe that the objectives of identifying victims of certain crimes and missing persons are laudable and, if they cannot be identified by other mechanisms, FRs would be a suitable technique for this purpose.

explain above, it leaves a wide margin of appreciation to the State when deciding which situations require the application of such a tool[797], which can lead to arbitrary actions.

In the latter case, the measure is restricted to the location or identification of specific individuals suspected of having committed a serious crime punishable in the State in question with a custodial sentence of at least four years. Such offenses, of course, include terrorism, along with others such as human trafficking, homicide, injuries, illicit organ trafficking, rape, etc.

In the latter two cases, as we have already pointed out, it is understood that exceptional measures may be adopted that are likely to limit the rights and freedoms of citizens, provided that they comply with certain requirements and specific safeguards established by law. In this sense, it is understood that they would be proportional and strictly necessary in a democratic society to achieve the maintenance of national security through the prevention and control of crime.

Similarly, the High Commissioner for Human Rights states that audio-visual and FR recording techniques should only be used when they meet the three conditions of legality, necessity and proportionality. Authorities should refrain from recording those attending meetings. Because of the need to respect the imperative of proportionality, exceptions can only be contemplated when there are concrete indications that serious crimes are being committed or there are grounds to suspect their imminence. Recordings should only be used for the identification of attendees at a meeting who are suspected of serious crimes[798]. Therefore, the measure must not exceed the limits of what is necessary and appropriate to achieve the intended purpose[799]. It discourages the use of this technique in peaceful assemblies, and governments that decide to implement it should ensure that they do so on a clear legal basis, including a strong regulatory framework that respects human rights and contains provisions that effectively protect personal data, in particular when dealing with facial images and data derived from them. Once collected, data should

[797] The margin of appreciation criterion differs between the CJEU and the ECHR. In the former it is limited, while in the latter it is broad because States are left to decide the best way to ensure national security and, consequently, the measure they consider most appropriate to achieve it. In this line, O'LEARY argues that if the current threats linked to terrorism and cross-border crime, as well as the increasing sophistication of technology, justify a very wide margin, the freedom given to governments with respect to the exploitation of the system must be more restricted in order to minimize abuse. O'LEARY, S. "La surveillance de masse et la Convention Européenne des Droits de l'Homme", in Lemmens, K. et al (Eds.), *Human Rights with a Human Touch. Liber amicorum Paul Lemmens*, Intersentia, Cambridge, 2019, pp. 267-268.

[798] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies*, cit., para. 35.

However, in the case of juveniles, consideration should also be given to age, minor culpability, the circumstances and needs of the child, as well as the diverse and long-term needs of society. In serious offenses committed by juveniles, measures must be proportionate to the circumstances of the individual and the seriousness of the offense, including considerations of the need for public safety and sanctions. See Committee on the Rights of the Child, *General Comment No. 10 (2007) children's rights in juvenile justice*, Geneva, 2007, para. 71.

[799] The case law of the CJEU is in this sense. See, for example, *Digital Rights Ireland Ltd* Judgment, para. 46.

be deleted immediately, except for specific segments that may be necessary in a criminal investigation and prosecution of violent crimes. All affected persons have the right to access and request the rectification and deletion of all information stored without a legitimate purpose and without legal basis, except when this operation may impede the development of an investigation or the initiation of criminal proceedings in which such data are necessary[800].

In order to contain the expansion of the FRs, the second paragraph of art. 5.h) AIA establishes that the measure must be triggered only when strictly necessary. It establishes a personal limitation as it adds that it may only be deployed to confirm the identity of the person specifically targeted. In addition, the nature of the situation must always be assessed, especially the seriousness, probability and magnitude of the harm that would result if the system were not used, as well as the consequences that such use would have on the rights and freedoms of those involved. Other temporal and geographical limitations must be considered and, likewise, before implementation, an assessment of the impact on fundamental rights must be carried out and registered in an EU database.

Once this process has been completed, its use may be authorized, which must be issued, as already indicated, by an independent judicial or administrative authority whose decision is binding on the State in question, to be issued upon a reasoned request and in accordance with the rules of domestic law, i.e., as provided by each country on the form and terms of use of the mechanisms[801]. In case of urgency, provided it is duly justified, this measure may be used without authorization and must be requested subsequently within a maximum period of 24 hours. In case of refusal, the mechanism must cease to be used immediately and all the data it contains must be deleted.

Authorization must always be granted on the basis of objective evidence or clear indications that the system is necessary and proportionate to achieve one of the exceptional situations in which its use is foreseen, specifying this in the authorization as well as that it is limited to what is strictly necessary in terms of time, geographical scope and personnel.

Despite the limits and specifics established by the AIA for real-time RBIS, we reiterate that we do not consider it to be a proportional or necessary measure in a democratic society such as ours, since the benefits are currently unknown, while the

[800] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies...*, cit., para. 36. Paragraph 37 establishes the need for well-structured and resourced monitoring mechanisms and additional measures; also that authorities need to be transparent and always notify citizens that they are being recorded or that their images could be processed by an FRs.

[801] Art. 5 h).1 AIA takes up this issue, stating that it is up to the States to decide whether to contemplate the possibility - in whole or in part - of using real-time RBIS, and that they must include in their domestic law the necessary detailed rules applicable to the request, granting and exercise of the authorizations, as well as monitoring and reporting. These rules must also specify the purposes and offenses for which the mechanisms are to be used. States may adopt more restrictive rules on their use, but in no case more lax than those provided for in the AIA.

interference in rights and freedoms is very high, to which must be added that there are less restrictive measures to ensure security and, in addition, we will have to wait to see how each State foresees the use of such measures. If this is the case with such mechanisms for which measures are established to limit their use, in the case of those that act in delayed mode, the situation is aggravated, since the way in which they are to be developed is not specified, and this may lead to a situation of massive surveillance of practically all citizens when they are deployed retrospectively. Therefore, we must answer the question posed in the negative. A similar view is expressed by KINDT, for whom continuous biometric comparison for investigative purposes in a public place does not meet the criterion of strict necessity in many times[802]. However, in spite of the above, in cases of identification of crime victims and missing persons, we consider that it could be very positive because it would be used only for the specific purpose of finding these persons but could run the risk of deriving in other different functions.

In conclusion, we consider that the provision made by the AIA on RBIS in public places for law enforcement purposes, whether delayed or in real time, is inadequate and its use will seriously jeopardize the rights and freedoms of citizens. The fact that the deployment of the latter is allowed, even though it is foreseen in three "exceptional" cases and always with the authorization of the competent authority (except for reasons of urgency), leaves the door open to the possibility of extending it to other situations under the argument of safeguarding an essential public interest, provided that there are alleged circumstances of urgency and necessity. Notwithstanding the above, the situation is even worse in the former because the specific cases and the safeguards and requirements to which they must be subject are not defined, which is why there is a risk, in extreme scenarios, of provoking a situation of massive and indiscriminate surveillance with the consequent intolerable impact on the rights and freedoms of the population[803].

[802] In the case of serious crime or terrorist attacks, it could be understood that the comparison, for a limited time, is strictly necessary if it is carried out with the appropriate safeguards to be defined in a law. KINDT, E.J. "Having yes, using no?", cit., p. 528. However, in our view, the fact that it is permitted in certain cases leaves the door open to extending it to other cases.

[803] This is because we are dealing with a technique capable of capturing the biometric data of the face of all persons in a given place without limitation, which represents a serious interference with the rights of citizenship, as reflected in paras. 56 and 57 of the CJEU Case C-594/12, *Digital Rights Ireland Ltd.*

V. OTHER PROBLEMS DERIVED FROM THE USE OF FACE DATA IN BIOMETRIC IDENTIFICATION SYSTEMS

1. Function creep

One of the problems or concerns raised by the use of FRs is that they may be used for purposes other than those for which they were originally intended[804]. This is known as function creep, defined by BREY as the "phenomenon by which a technology designed for a limited purpose may gain additional, unanticipated purposes or functions"[805]. MORDINI/MASSARI add that this purpose is usually "unintended or unauthorized"[806]. Function creep can have two origins: institutionalized expansions of its purposes or systematic abuses[807]. Although it may seem innocuous on some occasions, it always has the potential to erode public confidence in the system, which is even worse when they occur intentionally[808].

Such entrainment not only affects the aims or objectives but also extends to individuals, because those affected are not only those who are sought or identified, but also all the people analysed[809] (or susceptible to being captured by the mechanism). Thus, police forces could start using such systems not only to identify individuals being pursued in a crowd, but also, for example, to perform routine analysis of the composition of such crowds in public places or to perform statistical analysis of facial prints in order to predict criminal activity, or to track people[810].

The function creep has also been linked to a change or extension in the databases used by the algorithm[811]. Thus, GUO/KENNEDY state that it is acquired from the training

[804] In this sense, among others, KINDT, J.E. "Having yes, using no?...", cit., p. 524. The author is concerned about any widespread use of technology without or outside of a clear regulatory framework. Not only that, but he also considers the collection of biometric data to be dangerous, because "once information is collected, such information will be used".

[805] BREY, P. "Ethical aspects of facial recognition systems in public places...", cit., p. 104.

[806] MORDINI, E. & MASSARI, S. "Body, biometrics, and identity...", cit. p. 490.

[807] BREY, P. "Ethical aspects of facial recognition systems in public places...", cit., p. 104.

[808] MORDINI, E. & MASSARI, S. "Body, biometrics, and identity...", cit., p. 490. The authors go on to point out that, in the context of biometric applications, two situations of *function creep* can be distinguished. When they are used beyond the limits for which the system was officially adopted and when they are used inappropriately to generate unauthorized information. In addition, biometric systems could be used to create details that are not relevant for personal recognition and could be exploited for unintended or unauthorized purposes.

[809] COTINO HUESO, L. "Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection...", cit., p. 362.

[810] Current CCTV already has the potential to perform such activities but could be intended to use the technology for crime fighting purposes and to improve the quality of life in some neighbourhoods. BREY, P. "Ethical aspects of facial recognition systems in public places...", cit. p. 105.

[811] *Ibd.*, p. 104. The author states that the databases used in London, Birmingham, Tampa and Virginia Beach only included data on criminals under arrest warrants, sex offenders and missing persons. However, they can easily be expanded with the use of existing databases such as driver's license data. Thus, it is easy to include new categories of people subject to monitoring such as people involved in minor infractions, political activists, etc.

sets and only coincides in accuracy with them and may be used to analyse new facial datasets (which would, in turn, cause problems in relation to the accuracy of the system, which would be reduced if it starts to be used with datasets other than those with which it was designed or trained). To illustrate this situation, they give the example of the aforementioned Clearview AI database, created by a private company in which data obtained from social networks is reused for law enforcement purposes. Another example of extension is when the algorithmic system uses one database to analyse another. Along these lines, they argue that it should not be used indiscriminately to analyse any database without technical, legal and ethical parameters[812]. Another example of a change in the function of databases would be that of Aadhaar in India[813], which was voluntary and for the purpose of providing individuals with a unique citizen ID. Shortly thereafter, collection became mandatory for other purposes such as receiving school meals or opening bank accounts. In addition, access was opened to numerous non-governmental entities in the private sector, clearly for different purposes[814].

Another way in which this function creep can occur is in relation to users. The systems, once developed, could be implemented by other people or institutions. Thus, the government of one city or country might ask the police force of another to use the system, or individual operators might want to use them for personal reasons[815]. Finally, there may be a change of domain, i.e., a modification in the area in which it is developed, such as, for example, changes of neighbourhood, moving from an urban to a rural area, or from public to private areas, or vice versa[816]. As can be seen, there are many ways in which this problem can appear, which is very difficult to avoid because new scenarios or

[812] GUO, Z. & KENNEDY, L. "Policing base don automatic facial recognition...", cit., pp. 407-409. The authors add more *function creep* situations. Specifically with the introduction of FRs there is an imperceptibility in the use of CCTV data sets. Traditionally, the recordings issued by these had been analysed manually by the police. However, this is now done automatically by such mechanisms. Thus, large databases of CCTV data have been included in the ML algorithms with which these systems operate. They also consider that this entrainment occurs when individuals give up their data or share it with others through their social networks. Furthermore, they understand that algorithms that are applied to analyse live image datasets for identity recognition alone constitutes a creep suspicious function.

For all these reasons, the authors conclude on p. 411 that *function creep* is clearly contrary to the principle of consistency of purpose in data processing. Not only does it directly violate the privacy of those, but it also endangers society as a whole by fostering a culture of authoritarian control of objects and eroding the culture of surveillance by consent of individuals. Undefined policies or unregulated procedures established to supposedly protect individuals from the associated dangers can be detrimental to rights and freedoms. In an increasingly data-dependent and anonymity-averse society, there is evidence that privacy is increasingly eroding in the balance between privacy and security. Such a situation can lead to a loss of autonomy for the data subject, compromising their ability to understand and control their use of personally identifiable images in the form of digital data. This is especially true when surveillance is covert and public discourse and consensus are lacking.

[813] This biometric identification project in India has been heavily criticized by activists who point to potential security, privacy and corruption risks. Apart from looking at the citizenry as numbers, the Indian government seems more interested in controlling the population than in maintaining security. AHMED, S.I. et al. "Privacy, security and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, p. 908.

[814] See, KINDT. J.E. "Having yes, using no?", cit. p. 524.

[815] BREY, P. "Ethical aspects of facial recognition systems in public places...", cit., p. 105.

[816] *Idem.*

situations will always appear in which it is considered necessary to implement FRs. However, it can be limited through regulation and guaranteeing the security of the mechanisms.

Returning again to the issue of entrainment in relation to purpose, although one of the limits of personal data processing is to set a specific purpose, with the use of FRs there is a risk that they may be extended beyond those initially intended[817]. This may be due to errors in operation and personal data may start to be used for different purposes, or databases may be illegally accessed to alter the way in which they operate[818].

In systems operating in real time as provided for in the AIA, the objectives are restricted to the three specific situations in which the prohibition of their use has no virtuality and a whole series of measures and requirements must be observed for their implementation, such as the need for prior authorization by the competent authority issued within a specific time period. However, it could happen that, with a wide margin of discretion, the agents decide to implement the system because they consider that there is an imminent threat or danger to security, bypassing this requirement and subsequently requesting such authorization. In such a case, the deployment of the system might not be covered by any of the three exceptional circumstances included in the AIA and be motivated by other purposes, thus producing this function creep problem.

If the scenario just described is worrisome, it is even more so in the case of mechanisms that operate on a deferred basis, since the situations in which they may be triggered are not specified. In this sense, it may even extend to less serious crimes. The only thing that recital 95 AIA merely indicates is that they must be used in a proportionate and legitimate manner when strictly necessary and selectively as regards the persons to be identified, location and temporal scope, from a limited set of video recordings obtained in a lawful manner. What is strictly necessary is not specified, producing a situation of uncertainty. The GDPR also does not establish any specific limits in relation to the purposes of biometric identification, nor does the LED, which gives a great deal of discretion to the authorities to determine when they are faced with a situation that requires the deployment of the facial recognition mechanism. We will have to wait to see under what circumstances the police use such systems in the hope that they will not be extended in an uncontrolled manner to situations that do not require it since, as this same recital points out, they should not be used in such a way as to produce indiscriminate surveillance.

[817] *Ibd.*, p. 104.
[818] FRA, *Facial recognition technology...*, cit., p. 25.

2. Mass surveillance state

The above is worrying because it could lead to the establishment of a mass surveillance state, understood as a particular case of the information state that seeks to identify and solve governance problems through the collection, comparison, analysis and production of information[819]. SARTOR notes some of its advantages, linked to efficiency in the management of public activity, coordination of citizen behaviour and risk prevention. However, he is concerned about the uncertainty of the future that lies ahead due to the controversies that arise. Thus, new forms of influence and control may emerge, aimed at enslaving citizens to the purpose and values of those who control the surveillance infrastructure[820]. As early as 2007, the *Comité Consultatif d'Éthique pour les Sciences de la Vie et de la Santé* expressed concern about the risk of hyper-surveillance brought about by the collection and use of biometrics in the name of protecting human beings[821].

Those who use FRs have great power over the rest of the population, which generates great imbalances between the two. The AIA echoes this issue in several recitals. Thus, in paragraph 59 it argues that the actions of law enforcement authorities involving certain uses of the AIs are characterized by a significant imbalance of power and can lead to surveillance, detention or deprivation of liberty, as well as have other negative effects on rights. Specifically for RBIS that act in real time, in 32, it argues that it is a technique that seriously encroaches on rights and freedoms and that, among other issues, can lead to a sense of constant surveillance that has the effect of indirectly deterring their exercise; and, in the case of those operating in delayed mode, in number 95, it states that their deployment cannot lead to indiscriminate surveillance; and, even more specifically with regard to the creation of FR databases based on the massive extraction of facial images from the Internet or CCTV, it states in number 43 that they aggravate the feeling of mass surveillance.

The effect of this type of systems has already begun to be felt and the potential for persuasive control has led to a change in everyday behaviour, defined today as a new digital panopticon, a control system that operates as a sort of collective "super-ego" to remotely condition individual behaviour. We also speak of "Big Brother" to describe the society endowed with mass surveillance of the citizenry that has been brought about by the multiplication of control mechanisms[822] . Thus, as KINDT states, innocent people have the risk of being identified in political or religious demonstrations, being tracked and monitored, controlled and manipulated or stigmatized as suspects or, at least, having that feeling[823].

---

[819] SARTOR, G. *L'Intelligenza artificiale e il Diritto...*, cit., p. 77.

[820] *Idem*.

[821] Comité Consultatif d'Éthique pour les Sciences de la Vie et de la Santé, *Biométrie, données identifiantes et droits de l'homme*, Avis nº. 98, 2007.

[822] COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit., p. 125.

[823] KINDT, J.E. "Having yes, using not?...", cit., p. 525.

Illustrative of what has just been indicated is the ECHR Judgement *Big Brother Watch and others v. The United Kingdom*[824] in 2021 (first case of mass electronic monitoring with mass interception of communications). In it, the Grand Chamber confirmed that the British system of mass surveillance that had been disclosed by Edward Snowden as of 2013 did not meet the requirements under arts. 8 and 10 of the Convention. The mass interception of communications and the acquisition of data from communications through service providers resulted in a situation of mass surveillance. It concluded that the right to privacy had been interfered with in the sense that it had not been limited to what was strictly necessary in a democratic society and that the minimum guarantees for limiting this right had not been observed, namely the provision in a national rule of the grounds on which mass interception may be authorized as well as the circumstances under which it may be carried out, etc. Thus, the Court leaves the door open for this type of indiscriminate surveillance to be carried out in Europe by law enforcement forces with the serious consequences that it entails, if certain requirements are met. In reality, such a form of surveillance should not be allowed.

More interesting to us is the conclusion of Judge Pinto de Albuquerque's dissenting opinion (para. 59), in which he states that the judgement profoundly alters the balance in Europe between the right to privacy and the interests of public security, as it endorses non-selective surveillance of the content of electronic communications and associated communications data and, worse, the exchange of data with third countries that do not have a level of protection comparable to that of the Council of Europe states. It goes on to note that this conclusion is further justified in light of the CJEU's categorical rejection of general access to the content of electronic communications, its clear reluctance to allow general and undifferentiated retention of traffic and location data, and its limitations on the exchange of data with foreign intelligence services that do not provide a level of protection substantially equivalent to that guaranteed by the Charter. On these three points, the Strasbourg Court lags behind the Luxembourg Court, which remains the beacon of privacy protection in the European Union[825]. He concludes in para. 60 by declaring his concern about the future that awaits us, verbatim, "for good or ill, and I believe for ill more than for good, with the present judgment the Strasbourg Court has just opened the gates for an electronic "Big Brother" in Europe. If this is the new normal

[824] ECHR *Case Big Brother Watch and others v. The United Kingdom*, 25 May 2021, nos. 58170/13, 62322/14 and 24960/15.

[825] We must bear in mind that the ECHR and the CJEU have different competences, since the former carries out an external a posteriori control of a case related to the violation of human rights established in the Convention, in Europe. Thus, it judges the elements of the case and the solution offered by the national courts. In the case of mass surveillance, it checks whether the guarantees and procedures provided are capable of preventing the abuse of power; and whether the right balance between the competing elements was respected. For its part, the CJEU, by means of a preliminary ruling, can intervene at a preliminary stage on which the national judge has not yet made a final decision. The Court gives an official interpretation of European Union law which the national court must apply in the specific situation. O'LEARY, S. "La surveillance de masse et la Convention Européenne des Droits de l'Homme", in Lemmens, K. et al (Eds.), *Human Rights with a Human Touch. Liber amicorum Paul Lemmens*, Intersentia, Cambridge, 2019, pp. 265-266. For this reason, each court performs different tasks in different contexts, albeit with a priori similar approaches.

that my learned colleagues in the majority want for Europe, I cannot join them, and this I say with a disenchanted heart".

DUBUISSON is also critical of the pronouncement and permission of mass surveillance in Europe, since he maintains that the ECHR accepts to resort to it without any evaluation of its concrete modalities of operation, without considering the criticisms of the numerous international reports and scientific contributions on its real effectiveness and without examining in depth the balance between the advantages and disadvantages for fundamental rights. What it does take into account, however, are the assessments of the British authorities. He goes on to harshly assert that the Court merely hides behind the formulation of formal procedural requirements, very flexible and with very uncertain concrete application as to their ability to prevent abuses and ensure effective control by the intelligence services[826]. Therefore, in its view, it has been extremely flexible in its analysis, accepting a lack of definition of the reasons justifying this practice and the criteria governing the processing of the data collected. Moreover, instead of the specifics of the measures having to be adapted to the safeguards, the reverse is true and, instead of the latter being strengthened, they have been reduced to adapt them to the former, insofar as they are considered vital for security. In this way, what is achieved is to increase the margin of appreciation of the State[827], which implies a decrease in the demand for accountability granted to it, by allowing mass surveillance and invoking the threat of terrorism, apparently without scrutiny[828]. LOCK also reproves the result reached in the judgement and considers that, if the Court does not impose more rigorous requirements in this area, the deficiencies will continue in the UK surveillance system, and may even lead to its expansion to other countries. There is thus a risk that the Court's surveillance jurisprudence will be a mere fiction of restraint rather than a serious avenue for seeking concrete safeguards against abuses of power[829].

Therefore, in our view, the power of state surveillance entails serious dangers and the Court has missed the opportunity provided by this pronouncement to establish strict requirements limiting the government's action in the scope of application of mass surveillance measures.

[826] DUBUISSON, F. "La Cour Européenne des Droits de l'Homme face à la surveillance de masse (obs. sous Cour Eur. Dr. H., Gde Ch., arrêt Big Brother Watch et autres v. Royaume-Uni, 25 mai 2021), *Revue Trimestrielle des Droits de l'Homme*, no. 129, 2022, p. 132.

[827] *Ibd.*, pp. 135, 139.

[828] Of this opinion, HUGHES, K. "Mass surveillance and the European Court of Human Rights", *European Human Rights Law Review*, no. 6, 2018, p. 597. On p. 589 of the same research, the author shows his concern, not only about this aspect, but also about the fact that the Court requires minimum safeguards of rights and refuses to expand them to respond to new surveillance capabilities, and the lack of deference to the right to privacy and private life. They are barely mentioned in any substantive sense in the pronouncement and there is little recognition of the threat that secret surveillance poses to democracy.

[829] LOCK, D. "Case Analysis. Form over substance: Human Rights Law's search for effective protections against the abuse of surveillance powers", *European Human Rights Law Review*, nº. 3, 2022, p. 309.

That the British government resorts to this type of mass citizenship with broad discretion can also be extracted from the case from which the judgement of the Spanish Central Criminal Court 2/2024 derives. The incident took place in July 2022. A young British man who was about to take a flight from London to Menorca, sent a prank message threatening to blow up the plane to his fellow passengers through a private group on the social network Snapchat. This message, along with a photograph, was intercepted by the British security services and this resulted in the mobilization of a Spanish Army Eurofighter to escort the plane to its destination. For this incident, the Spanish Prosecutor's Office of the National Audience and the Spanish State Attorney's Office requested a fine of 22,500€ for a crime of public disorder, as well as a civil liability compensation of 94,782€ in favour of the Ministry of Defence for the cost of mobilizing the aircraft that escorted the plane. Once on the ground, it was verified that the threat was not real as there were no explosives or objects or instruments to confirm it. After analysing the case and the typical elements of the crime of public disorder as provided for in the Spanish Criminal Code, the central criminal judge concluded that this action cannot be considered to constitute a crime[830]. A central issue in this particular case is that the sending of the message and the photograph was done through a private channel of the social network indicated and was not sent to any official body or given any publicity, which is why we understand that the privacy of the individual was violated. For this reason, the central criminal judge considers that the defendant could not assume that his communication could be intercepted or detected by third parties outside the group of friends to whom he addressed the message, not even the British security services. The ruling continues by pointing out that the transmission of a message through a private group of a social network is not equivalent to public dissemination, so that the expectation of privacy that one has when private communications are made was annulled[831] and, for this reason, we reiterate, there was a violation of the right to privacy of the young man.

Returning to the issue that concerns us, that is, the use of FRs, we must point out that those that operate in real time can be used when there is a serious threat to the security and life of people. If, as in the situation just described, the threat is not real and the measure is triggered or even the detention of a suspected individual has been derived, there may be a serious violation of the rights of citizens that would even lead to the deprivation of liberty and the initiation of criminal proceedings.

The impact of FRs on surveillance cannot be underestimated because it can lead to uncontrolled and massive surveillance of citizens. The search for security and the fight against terrorism as one of the legitimate objectives that allow the restriction of rights,

[830] COMMUNICATION PODER JUDICIAL, *La Audiencia Nacional acquits British youth tried for sending message during flight threatening to blow up plane*, 25 January 2024. Electronic resource obtained via the World Wide Web: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-absuelve-a-un-joven-britanico-juzgado-por-enviar-un-mensaje-durante-un-vuelo-en-el-que-amenazaba-con-volar-el-avion-, [retrieved on 28 August, 2024].

[831] Sentencia Juzgado Central de lo Penal 2/2024, 23 January 2024, [JUR 2024/49366]. ECLI:EN:AN:2024:388.

has resulted in the threat to privacy by the "securitization" of dangers such as the one mentioned above, at the expense of sacrificing other basic aspects and leading to situations of social inequality and global injustice, since "securitization" is a political framework that allows the breaking of rules[832].

Along these lines, FRs allow authorities to immediately identify who is present at a given location, who they are with and what they are doing. Such an ability can be applied in real time but can also be done by analysing an already recorded CCTV image. The latter allows retrospective monitoring of social movements and is able to locate specific individuals[833]. Not only that, but it allows to observe an entire population. The state's ability to locate individuals allows them to be monitored and profiled, which increases the potential for surveillance linked to FR[834]. This undermines the ability of individuals to live and act anonymously, altering their way of life and producing an imbalance of power between the state and individuals.

In this regard, the High Commissioner for Human Rights notes a worrying trend that may result in public spaces being systematically monitored by cameras and FRs. States must exercise human rights due diligence not only before deploying the devices but throughout their life cycle[835], in order to avoid a situation of mass surveillance that severely impairs the ability to live in society and the exercise of essential rights and freedoms.

However, we should point out that it is not only the government that exercises control over individuals through the power granted by new technologies and, more specifically, AIs, but also the citizens themselves. Thus, control today is not only vertical, but also horizontal. The Internet and social networks act as systems of social control. In a hyperconnected context such as the one we live in, it is the very people susceptible to control who can become controllers in turn. Thus, the community is immersed in a culture of surveillance[836]. There is a constant traceability of human life through data and, of

[832] RUSINOVA, V. "Privacy and the legalisation of mass surveillance: In search of a second wind for international human rights law", *The International Journal of Human Rights*, vol. 26, nº. 4, 2022, p. 743. The author distinguishes two types of data analysis: subject-based and pattern-based. The former are implemented when there is a specific threat and do not require the massive interception of data and can be implemented through a type of individual surveillance, subject to legal safeguards. The latter, on the other hand, do require the collection of huge amounts of data.

[833] Conventional video surveillance systems already allow the surveillance of all citizens, resulting in a very high level of social control, from the moment in which they allow the retrospective review of the video materials derived from them because they are stored for a period of time. Therefore, LECHNER understands that they go from being a preventive instrument to a repressive one when these images are used to individualize those suspected of having committed a crime from the rest of society. LECHNER, M. "Technologies applied to citizen security: challenges for transitional justice in the face of new mechanisms of social control", *Divulgation*, vol. 1, nº. 1, 2016, p. 5.

If, as we say, with such mechanisms there is a risk of mass surveillance, even more so when FRs are inserted into them, since they favour the monitoring of the entire citizenry and the immediate detection of the individual being searched.

[834] MURRAY, D. "Facial recognition and the end of human rights...", cit., p. 148.

[835] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies*, cit., para. 38.

[836] COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit., p. 126.

course, the FRs is inserted in this scenario, in which the human face is reduced to a set of disaggregated data and used for the most diverse purposes[837], the one that concerns us, security. Thus, such indiscriminate mechanisms are being installed in video surveillance devices in public spaces, with the particularity that the processing of face data they perform in this case cannot be based on the express consent of the interested parties.

In view of the above, it is necessary to address the aspects that revolve around the potential offered by FRs to LEAs in terms of security and crime control, analysing the possible risks arising from this in the scenario of mass surveillance and monitoring that we have introduced at this point.

[837] Of this opinion, *Idem*.

CHAPTER IV

POLICE ROLE IN MAINTAINING SECURITY AND THE RISK OF MASS SURVEILLANCE ARISING FROM THE USE OF FACIAL RECOGNITION SYSTEMS

I. APPROACH TO THE TERM SECURITY

To begin this last chapter of our research, dedicated to the analysis of the expected benefits of FRs in terms of security and the risks of deriving in a situation of mass surveillance, it is necessary to specify what is meant by mass surveillance and the different terms used to describe it.

This is a concept that has evolved over time[838]. In recent decades it has done so at a dizzying pace, motivated by the process of profound reconfiguration of the international order since the implosion of the USSR put an end to the bipolarity that emerged after World War II. That was a scenario that could be called "simple" in comparison with the current one. Two ideologically opposed blocs, with no economic, cultural or technological ties, challenged each other in terms of warfare. In that context, the term security was identified with defence. However, this simplistic vision does not hold true today and the scope of the term has been transformed to include human security[839]. Likewise, the idea of security has a multifaceted and complex, multidimensional and changing meaning[840]. This can be seen, for example, in the *Report of the United Nations Millennium Summit* in 2000, where the Secretary General of the United Nations stated that the concept of security was "synonymous with the defence of territory against external attacks". He adds, however, that "the demands of security have meant that today it also encompasses the protection of communities and individuals from various internal acts of violence"[841]. For this reason, the definitions that have been tried and tested are very diverse.

In spite of the above, what is certain is that security is the cornerstone of society, since it enables the development of community life in a peaceful and orderly manner. In addition, it is a condition and transversal foundation that structures contemporary forms of organization. In this sense, ACOSTA GUZMÁN understands it as "a condition and ideal end that allows human beings to act with their environment, individually or collectively"[842]. For this reason, it enables every person to achieve his or her fulfilment

[838] BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública", *IUS. Revista del Instituto de Ciencias jurídicas de Puebla, Mexico*, vol. 13, nº. 44, 2019, 2019, p. 254. Some of the transformations experienced have been public, social, legal, human and citizen security, among others.

[839] DACOBA CERVIÑO, F.J. "Prólogo" to FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es) en un futuro incierto (un estudio jurídico constitucional)*, Aranzadi, Navarra, 2020, pp. 13-14. The author of the prologue advocates the use of this broad term on p. 46.

[840] FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es) en un futuro incierto (un estudio jurídico constitucional)*, Aranzadi, Navarra, 2020, p. 31.

[841] ANNAN, K. '*We the Peoples'. The Role of the United Nations in the 21st Century*, United Nations Millennium Summit, 2000. Electronic resource obtained via the World Wide Web: https://www.un.org/es/events/pastevents/millennium_summit/sg_report/full.htm, [retrieved 20 December 2023].

[842] ACOSTA GUZMÁN, H.M. "Lineamientos estratégicos para combatir los Grupos Armados Organizados en el escenario pos-acuerdo", in Payá Santos, C.A. (Dir.), *La gestión del riesgo. La inseguridad jurídica y las amenazas a la seguridad*, Aranzadi, Navarra, 2020, p. 108.

in any social environment, as long as the scenario is adequately based on justice, order and stability, avoiding conflicts that prevent or hinder his or her full development[843].

There are different connotations of security: public, citizen, State[844], national[845], etc. The first two are the most interesting for the purposes of our study insofar as they refer to the maintenance of the security of society, threatened by crime. Both terms are usually considered as synonyms[846], although they present some nuances (which is why we will refer to them interchangeably as security), as stated in the Preamble of the Spanish Organic Law 4/2015, of March 30, on the protection of citizen security, which understands by both "the activity aimed at the protection of persons and property and the maintenance of public tranquillity". So that security is linked to the "guarantee that the rights and freedoms recognized and protected in the democratic constitutions can be freely exercised by citizens and not mere formal declarations lacking legal effectiveness"[847]. Therefore, it is one of the fundamental elements of the rule of law.

[843] *Idem.* The author goes on to point out that security is not exclusive to the military and police sphere, because it is the responsibility of all citizens. Defence thus consists of establishing, strengthening and generating an environment free of dangers, internal and external threats or situations that directly or indirectly threaten the common national interests. It is about avoiding any scenario by using the necessary means and capabilities to achieve these objectives in all areas of the State. Therefore, security should not be framed in the classical perspective that prioritizes coercive means and the use of force, but rather, it depends on the field of action in which social dynamics are developed, from which the means available to achieve security are contemplated. For this reason, all sectors of the State, whether public or private, must be oriented towards achieving this higher good.

[844] This type of security is aimed at protecting the assets and interests of the State that cannot be renounced, either through the identification of the threats or dangers inherent to such interests, or through the measures to be adopted to maintain, develop and defend them. These are, on the one hand, actions directed outwardly in political, diplomatic, economic and financial sectors; and, on the other hand, preventive and repressive measures for internal situations within the national territory that seriously endanger the functioning or survival of the institutional organs. DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica. Profili ricostruttive e applicative*, G. Giappichelli Editore, Torino, 2010, p. 18.

[845] This is a broader concept that encompasses all of the above. As established in art. 3 of Law 36/2015, of September 28, 2015, on Spanish National Security, it refers to state action aimed at protecting the freedom, rights and welfare of the population, guaranteeing the defence of the national territory as well as its principles and values. It transcends this regional scope as it also aims to contribute to international security together with other partner and allied countries.

HIRANANDANI, V. "Privacy and security in the digital age...", cit., p. 1101 considers that human and national security are not exclusive and reinforce each other, being complementary.

[846] For his part, LECHNER considers that they are different terms because citizen security surpasses public security. LECHNER, M. "Tecnologías aplicadas a la seguridad ciudadana...", cit., p. 4.

[847] This is also the position of the doctrine. See, FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es)...*, cit., p. 38; DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica...*, cit., p. 23. The latter understands security as a de facto situation whereby a community of individuals lives in conditions of equilibrium and harmony in a given territorial area. Thus, this situation is characterized by the absence of impediments to the enjoyment of this balanced harmony. Therefore, he relates it to the quality of life of a community in its own territory.

Jurisprudence distinguishes between security in the strict sense and security in the broad sense. From the former, security is the activity aimed at the protection of persons and property, while the latter refers to the maintenance of tranquility or public order. Both are inseparable and mutually conditioned purposes. Sentence SCC 33/1982, 8 June 1982, in its Legal Ground 3.

The State is in charge of its maintenance[848], eliminating violence and obstacles to the free exercise of the rights and freedoms of citizens. One of the elements at its disposal to guarantee their adequate protection are the LEAs, together with the existence of a legal system suitable for responding to illicit phenomena of any kind and a judicial power that ensures its correct application.

As stated in the Preamble of Spanish Organic Law 2/1986, of March 13, 1986, on Security Forces and Corps, it is difficult to precisely delimit all the factual realities susceptible of endangering it, given that they are forecasts of the future for which the time, place, importance and, in general, the circumstances and conditions of their appearance are unknown. However, not everything that is understood as safety –for example, in transportation– is included within the term safety in the sense that concerns us. Along similar lines, Judgement of the Spanish Constitutional Court 59/1985, 6 May 1985, in its Legal Basis 2, holds that not all security of persons and goods, nor all regulations aimed at achieving it or preserving its maintenance, can be included in the same because, if so, practically all the rules of the legal system would be rules of public security and, therefore, State competence, when on many occasions the task of ensuring it is carried out at the local level. We are therefore dealing with a more restrictive concept that refers to the functions of the LEAs and the instrumental means to carry them out[849].

[848] Along these lines, KIKLAS/BARRERA understand public security as a service to be provided by the State to guarantee the integrity of the entire population and its property. NIKLAS, P. & BARRERA, G. "Biometría aplicada a la seguridad pública...", cit., p. 146.

[849] A concept of security that would include all aspects of security in a broad sense would be that of human security. It is a more dynamic category than that of citizen/public and, from a social approach, it is considered more inclusive and in line with the guarantee of a dignified life for people that public systems should pursue. A true establishment of fundamental rights that does not remain only formalisms, in theoretical regulations without guarantees, requires this type of security, which is centered on people (as opposed to States) and is built from their interests, designed taking into account the citizenry in order to make them feel more secure, in the sense of matching the demands for security with what is really needed. FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es)...*, cit., pp. 48-50. Thus, it is a concept that encompasses human rights, environmental protection and guarantees the basic needs of health, education and personal security. ZUREIK, E. & HINDLE, K. "Governance, security and technology: the case of biometrics", *Studies in Political Economics*, vol. 73, nº. 1, 2004, p. 114. Similarly, BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública...", cit., pp. 255-256. The latter argues that the welfare of the people is placed as the main objective of this security model, linked to the treatments associated with public force, maintenance of law and order, as well as the eradication of violence and insecurity.

The main objective of human security is to extend the concept of security beyond national security, as the only way to force the state to pay more attention to the needs of its population. The term security is used to persuade rulers that citizen security coincides with state security because, if the population is insecure, so are states. Moreover, the term implies that the latter can be negatively affected by the insecurity of the population outside their own borders. On the other hand, one of the novelties introduced by this concept of security refers to the obligation of the international community to protect people when their states are unable to do so. Thus, human security goes against threats to humanity. HOWARD-HASSMAN, R.E. "Human security: Undermining human rights?", *Human Rights Quarterly*, vol. 34, 2012, p. 90.

The term human security began to be used in 1994 in the United Nations Development Programme's *Human Development Report 1994*, pp. 1-10. The concept equates security with people and development rather than linking it to territories and weapons. It is the right of people to make secure and free choices, confident that they will have the same opportunities in the future as they have in the present. For this reason, security is identified with well-being at all levels and the defence of human rights and fundamental freedoms. In the same text, specifically on p. 50, reference is also made to natural security as

The latter are not limited to those aimed at preventing and punishing crimes, since they are of very diverse typology and their ultimate goal is to create a citizen perception of security that allows a high quality of life for society and the enjoyment of the spaces of a territory at all times, in conditions of tranquillity and freedom[850].

A concept linked to security is that of public order[851] which includes the security of persons and property as well as that of the State itself[852]. The term refers to the repression of crimes, criminality, minimization of delinquency, etc. It is also a state competence and a necessary and sufficient condition for citizen security, in the sense of protecting the population from those who attempt to carry out acts that infringe the rules[853] , through the establishment of conflict resolution channels[854]. Thus, public order can be understood in the sense of peace, tranquillity and security, not only of the State, but also of individuals (hence its public nature). In the criminal sphere, it is linked to the proper functioning of punitive justice and its alteration is manifested through the criminal offense executed or potential[855].

Public order is a good of a collective nature that acts as a general limit to other rights. Thus, for example, art. 16.1 of the Spanish Constitution guarantees ideological, religious and worship freedom in all its manifestations, restricting its exercise only when it infringes upon it. In Italy it is also considered an inherent good of the constitutional

---

a methodological and scientific requirement, like the previous one, to be able to face the environmental problems that affect us.

[850] DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica...*, cit.,p. 180. Similarly, BAJC, V. "Sociological reflections on security through surveillance", *Sociological Forum*, vol. 28, nº. 3, 2013, p. 616. The latter argues that security is a perception of reality by individuals, social groups and institutions that tends to be internalized as a feeling or emotion and articulated politically as an ideology or agenda. It is thus considered a perception of the social world with profound consequences on the way of daily life.

[851] However, when it comes to understanding the police function, although linked, we must bear in mind that security and public order are two different concepts, since the latter refers to the guarantee of the order previously established by the organs of power, while the former seeks to guarantee the rights and freedoms of citizens and their peaceful coexistence. JAR COUSELO, G. "El papel de la Policía en una sociedad democrática", *REIS. Revista Española de Investigaciones Sociológicas*, nº. 85, 1999, p. 208.

[852] KATROUGALOS, G. "The tension between personal freedom and security from risks", *Annuaire International des Droits de l'Homme. Conflicts de Droits de l'Homme*, vol. 4, 2009, p. 220.

[853] CEPEDA HERNÁNDEZ, A.J. "Garantías de la seguridad ciudadana en el marco del apoyo de las Fuerzas Armadas a la Policía Nacional de República Dominicana en un marco de Seguridad y Defensa", in Payá Santos, C.A. (Dir.), *La gestión del riesgo. La inseguridad jurídica y las amenazas a la seguridad*, Aranzadi, Navarra, 2020, p. 133.

[854] In this line, the maintenance of order in a democratic society should be understood as the balance between the different social forces and the establishment of channels for conflict resolution. MARTÍN FERNÁNDEZ, M. "Policía, profesión y organización: Hacia un modelo integral de la policía en España", *Revista Española de Investigaciones Sociológicas*, nº. 59, 1992, p. 208. As the author points out, the above implies both the exercise of authority to dictate rules that make coexistence possible and social legitimization to achieve broad acceptance of them, and the establishment of a formal social control apparatus to prevent any dysfunctions that may occur. It also highlights as the last essential part of this social control apparatus, the legitimate use of force, delegated to the police.

[855] In addition to the criminal definition, there is another normative definition, by which it is understood that the order is granted by an authority. Thus, public order is characterized by a set of rules inspired by considerations of general interest, which is why it must be enforced. CERF, A. "Ordre public, Droit pénal, et droits fondamentaux", in Redor, M.J (Dir.), *L'ordre public: Ordre publico u ordres publics? Ordre public et droits fondamentaux*, Bruylant, Brussels, 2001, p. 64.

system and the provisions dictated for its protection cannot be hindered by other rights[856]. Despite what we have just pointed out, public order is not absolute and also finds its own limits, in this specific case, in the exercise of rights and freedoms[857]. The pre-eminence of one over the other will have to be assessed in the specific case, in a weighing of interests.

The community expects a generalized respect for the rules of coexistence, and therefore demands from the institutions a real security that goes beyond the subjective perception of it[858]. In this sense, security is shown as a situation of serenity and tranquillity that makes citizens feel free to go about their daily lives[859]. Threats to security are ever-changing and, nowadays, the problems are particularly intense, to the point that modern society is considered as a "risk society", where future incidents are of great concern, causing a feeling of anxiety in the population[860].

Terrorism (as we discussed in Chapter I) and the various forms of serious crime pose a serious threat to security. Globalization contributes to aggravating the problems by fostering large-scale criminal phenomena, making them global threats that transcend all state boundaries. This has a major impact on security, since global threats tend to be of greater intensity and attack fundamental rights with greater force in interconnected geographical areas, while crime increases its potential for harm[861]. Another element that threatens security (linked to the previous one) is ICTs, as they modify borders and fields of action[862], as well as allowing the emergence of new forms of crime committed through them. However, this tool is not used solely for the purpose of crime, as it is also used for surveillance purposes. In this sense, it appears as an opportunity and is being used at government level, on many occasions, in an intrusive way, as it allows the monitoring, scanning and analysis of large amounts of data. Citizens tend to justify measures that

[856] DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica ...*, cit.

[857] More extensively, *Ibd.*, pp. 113-117. Likewise, JAR COUSELO, G. "El papel de la Policía en una sociedad democrática...", p. 210, p. 210. The latter argues the need to reconcile justice, understood as the assurance of rights and liberties, with order, i.e., with the repression of behaviors that threaten security; & CARVAJAL MARTÍNEZ, J.E. "El paradigma de la seguridad y las tensiones con los derechos humanos", *Utopía y Praxis Latinoamericana*, vol. 23, nº. 1, 2018, p. 104, when he argues that States have the obligation to establish security policies that incorporate human rights standards as a limit for the intervention of state forces.

[858] DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica...*, cit.,, p. 113.

[859] *Ibd.*, p. 180. For the aforementioned author, security depends very much on the subjective sensation that citizens have of it, which is why he believes that it is part of the social perception that varies from period to period. Similarly, TAVAREZ-ALVARADO, H.A. et al. "Factores de riesgo en la violación de derechos humanos por parte de policías", *Ratio Juris*, vol. 19, nº. 38, 2024, p. 4.

[860] KROENER, I. & NEYLAND, D. "New technologies, security and surveillance", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 143.

[861] BERNAL DEL CASTILLO, J. "Prevención y seguridad ciudadana. La recepción en España de las teorías criminológicas de la prevención situacional", *Revista de Derecho Penal y Criminología*, nº. 9, 2013, pp. 268-269.

[862] LECHNER, M. "Tecnologías aplicadas a la seguridad ciudadana...", cit., p. 3.

facilitate this type of surveillance if they are used to fight against serious threats such as terrorism and society considers them appropriate for this purpose[863].

Thus, the new threats not only cause an increase in crime rates and, therefore, objective insecurity, but also a decrease in the subjective perception of security –as indicated above– often promoted by certain sectors in power[864]. In order to keep the latter high, society demands greater intervention from the State through the implementation of new security policies, especially through recourse to criminal law and the adoption of preventive measures[865], in order to address the risks and avoid an increase in criminal behaviour[866]. However, Western societies are immersed in a process of overprotection of the citizenry, driven by the fear of the terrorist threat and the idea that only through new

[863] REDDICK, C.G. et al. "Public opinion on National Security Agency surveillance multi-method approach," *Government Information Quarterly*, vol. 32, 2015, p. 220.

[864] CARVAJAL MARTÍNEZ, J.E. "El paradigma de la seguridad y las tensiones con los derechos humanos...", cit., p. 98. Such as, for example, the media or the State itself, in order to legitimize the adoption of new measures that can be very restrictive of rights and freedoms, with the aim of controlling criminal events that supposedly seriously endanger security. In this regard, GATES provides a broad overview of the situation in the United States following the attacks of September 11, 2001. In the aftermath of the attacks, a campaign was launched to combat terrorism by implementing FRs and creating databases and terrorist watch lists. In order to implement them, it was necessary to count on the support of citizens, who offered it in exchange for feeling safer against the diffuse, global threat posed by international terrorism. In the author's opinion, what really happened was a racialization of the enemy because a racial image of the enemy was constructed and spread through the media. GATES, K.A. *Our biometric future...*, cit., pp. 97-124. LYON/WOOD speak of a situation of "management insecurity" provoked by different public and private transnational agencies. This process of "(in)securitization" is manifested in the use of surveillance technologies that impact on everyday life. So that routine bureaucratic decisions, real technologies and continuous technological rationalization operate together as an apparatus that favours the aforementioned process. LYON, D. & WOOD, D.M. "Security, surveillance, and sociological analysis", *Canadian Review of Sociology*, vol. 49, no. 4, 2012, p. 320.

[865] BERNAL DEL CASTILLO, J. "Prevención y seguridad ciudadana...", cit., p. 269. Society today has security as one of its main concerns, and therefore demands its adequate maintenance. BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública...", cit., p. 252. Similarly, FERNÁNDEZ RODRÍGUEZ, when he states that, at present, given the emerging threats and risks, security is placed as a priority in public agendas. This situation is especially motivated in Europe by jihadist terrorism which, due to its operational capacity, has provoked the pressure of insecurity FERNÁNDEZ RODRÍGUEZ, J.J. "El encuentro entre seguridad y derechos humanos...", cit., p. 89. The unpredictability of these events, which can produce disproportionately large effects, greatly increases the sense of urgency when intervening. This serves to justify the systematic collection of data and the use of data-mining to reconstruct the patterns of such incidents in order to analyze them for future prevention. BAJC, V. "Sociological reflections on security through surveillance...", cit. p. 619.

[866] BUSTOS RAMÍREZ criticizes the fact that crime prevention is reduced to a feeling of security. He argues that the police usually act once the criminal offense has been committed and must do so because they do not know where and when it will be committed. This approach can be qualified today by the advance of technology, given that with new crime prediction mechanisms it is possible to know with a certain degree of certainty when criminal events may occur. However, we agree with the author in considering that preventive vigilance could lead to the displacement of punishable conducts to other sectors, causing a greater feeling of insecurity. BUSTOS RAMÍREZ, J. "Las funciones de la policía y la libertad y seguridad de los ciudadanos", *Nuevo Foro Penal*, nº. 32, 1986, pp. 167-168.

Extrapolating the above to the deployment of FRs, we understand that it could lead to the displacement of crime to areas that are not subject to surveillance by these mechanisms, unless they are implemented covertly and individuals are not aware of it, which in the case of crime prevention will be the most frequent situation.

crime control technologies is it possible to carry out effective surveillance[867]. Thus, the latter have included explicit efforts aimed at measuring and managing levels of public fear and insecurity. Therefore, GATES considers that efforts are being made to modify public perception, rather than to combat crime[868].

Among these measures are technological innovations that, along with the benefits they bring, lead to an increase in threats and situations that endanger security, damaging fundamental rights[869], sometimes constituting disproportionate responses[870]. Among these new instruments deployed to address the public's fear of crime and to try to control it, are the FRs inserted in the CCTV, since part of their work is symbolic, linked to the authority (also symbolic) of the LEAs[871]. With the inclusion of such techniques in the fight against terrorism and serious crime, as MARCUS/MILLER argue, there is a risk that their use will become widespread and continuous, reaching general crime, when in the latter case it is unnecessary and totally disproportionate[872].

Throughout this Chapter, different issues related to the exercise of the police function of maintaining security, the existing debate between freedom (and the consequent exercise of rights and freedoms) and security will be addressed, as well as the new trends in relation to social control and its link with the dystopian society and the panopticon.

---

[867] VERMEERSCH, H. & DE PAUW, E. "The acceptance of new security oriented technologies", in Friedewald, M. et al (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, p. 52.

[868] He further adds that crime prevention strategies assume high crime rates as normal, allowing criminal justice systems to experiment with new ways of managing crime rather than assuming that it can be reduced by managing the social conditions it produces. GATES, K.A. *Our biometric future...*, cit., pp. 68-69.

[869] DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica...*, cit. pp. 2-3. The author argues that, for this reason, there has been a change in security, which has acquired new connotations since the authority is omnipresent and tends to limit, under the argument of security, the inviolable sphere of individuals, because some interventions that are objectively restrictive of rights and freedoms are subjectively and collectively perceived as functional for the protection of freedom.

The same author, on p. 4, maintains that security is a locution that derives from a psychological situation linked to the absence of dangers, to which relevance is given to the point of consenting public authorities to limit the exercise of individual freedom. To guarantee it, preventive and repressive measures are adopted.

[870] In the opposite sense, LYNCH, N. "Facial Recognition Technology in Policing and Security...", cit. For the author, the use of emerging technologies such as FRs can sometimes be a proportionate response in situations where the community or individuals are at risk.

[871] GATES, K.A. *Our biometric future...*, cit., p. 69. However, as stated in the cited work, it would be a mistake to consider that FRs have a merely symbolic function.

KROENER, I. & NEYLAND, D. "New technologies, security and surveillance...", cit., pp. 143-144, state that, on many occasions, the effect achieved by the implementation of surveillance measures is the opposite, i.e., to increase the feeling of insecurity instead of reducing it.

[872] Thus, from the context of anti-terrorist security (emergency) derives an endless "war" against serious crime, which in turn is transformed into an endless war against general crime. MARCUS, S. & MILLER, S. *Biometric identification, law and ethics...*, cit., pp. 33-34.

II. POLICE FUNCTION OF MAINTAINING SECURITY IN A DEMOCRATIC STATE

Some of the characteristic features of democratic society are the recognition and respect for the rights and freedoms of the population, as well as the protection of the just requirements of morality, public order and general welfare, which can be achieved in part through the police, who enforce the law by trying to prevent crime[873]. It is the State that has the duty to preserve it, which includes, as stated by the CJEU, the prevention and repression of activities that may seriously destabilize the fundamental constitutional, political, economic or social structures of a country and, in particular, directly threaten society, the population or the State itself, in particular terrorism[874]. The guarantee of security is carried out through the police, which is why it is considered as a public service of protection[875] and an essential part of the state intervention on the population in relation to an effective control. For this reason, it also has the power to limit rights. Thus, the police is the immediate supervisory body (the most specific aspect of state control and intervention in society) and one of the most important of control in general[876]. For this reason, BUSTOS RAMÍREZ links the police with rights and states that it would be meaningless to speak of these if they were not related to the police function[877].

Thus, the State has the obligation to guarantee community life and equal rights[878]. It has a monopoly of force exercised through the police as the institution responsible for ensuring security, for which it has broad powers of prevention, control and coercion. It has the capacity to limit rights if this protects the citizenry[879], but it must also respect them, since they are also one of the limits it must observe in its actions[880]. This means that police functions and the measures available to them for their exercise cannot be used to justify disproportionate and illegitimate interference with fundamental rights[881]. On the other hand, any police action carried out in the exercise of their duties must always meet

[873] CRAWSHAW, R. "Introduction to the seminar on human rights and the police...", cit., p. 13.

[874] *La Quadrature du Net*, para. 135.

[875] JAR COUSELO, G. "El papel de la Policía en una sociedad democrática...", cit., p. 215.

[876] BUSTOS RAMÍREZ, J. "The functions of the police and the freedom and security of citizens...", cit., p. 165.

[877] *Idem*. He goes on to point out that a neutral or technical inquiry into the police function that does not connect it to the political system means overlooking rights and disregarding the Constitution.

[878] MARTÍN FERNÁNDEZ, M. "Police, profession and organization...", cit., p. 208.

[879] *Ibd.*, p. 207, 208. The author maintains that the limitations of individual freedom to make life in common possible can only be administered by the State.

[880] BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública...", cit., p. 263. ALLEWELDT, R. & FICKENSCHER, G. "Introduction: The police, a key actor in human rights protection", *The police and international human rights law*, Springer, 2018, p. 2.

[881] JAR COUSELO, G. "El papel de la Policía en una sociedad democrática...", cit., p. 215. The author states that, in a democratic system, the maintenance of order is a balance between social forces and the establishment of channels for the resolution of conflicts that are inherent to any complex society.

the permitted normative criteria and the preservation of human dignity[882]. The latter, as the source from which all other fundamental rights and freedoms emanate.

The above does not extend to authoritarian regimes, in which the police are inspired by military principles, among which are obedience, hierarchy or discipline; and their activities tend to be of control of social activities, manifesting themselves with greater rigor in the maintenance of public order[883]. For JAR COUSELO, the fact that the police in this type of State follows a military model serves to maintain social loyalty to it, but it is not the most adequate to guarantee the free and peaceful exercise of rights and liberties. On the contrary, to ensure the latter, a general climate of order, tolerance and peace is needed in which the police are a basic element of the homogeneous whole in which it is possible to achieve greater levels of efficiency with less risk to freedoms[884].

On the contrary, in a democratic state, the objective of the police is the defence of the law and of the norms dictated in order to maintain social order, since rights cannot be exercised without that[885]. To this is added the search for social equilibrium and common welfare, in order to promote citizen cohesion. At the same time, it also acts to control the exercise of state power[886]. All of the above implies the resolution of problems in conflict situations and their prevention, always seeking balance in its actions[887]. Thus, the police not only have a repressive function against crime, but also a preventive one[888] in order to guarantee security and, consequently, the exercise of rights and freedoms to the maximum extent possible. Both tasks are essential because if the penal system were based solely on absolute prevention, there would be a risk of becoming a police state, contrary to the former, and based on the submission and obedience of the citizenry, so that control would lack legitimacy[889]. Moreover, despite the name, it is considered the antithesis of the police because States use this power disproportionately or for the benefit of a few and not of the

[882] BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública...", cit., p. 267. The author reaches this conclusion after explaining the limits that must be observed in the exercise of force by the police, that is, the criteria of proportionality and necessity.

[883] JAR COUSELO, G. "The role of the police in a democratic society...", cit., pp. 204-205.

[884] *Ibd.*, p. 205.

[885] CRAWSHAW, R., "Introduction to the seminar on human rights and the police...", cit., p. 15. Social order, for the author, is characterized by tolerable levels of crime and low levels of social tension, and this depends to a large extent on effective policing.

[886] ALLEWELDT, R. & FICKENSCHER, G. "Introduction: The police, a key actor in human rights protection...", cit. p. 8.

[887] MARTÍN FERNÁNDEZ, M. "Policía, profesión y organización...", cit., p. 209.

[888] These are two sides of the same coin of police functions. MURDOCH, J. "Police powers and criminal investigations", in Alleweldt, R. & Fickenscher, G. (Eds.), *The police and international human rights law*, Springer, 2018, p. 127. The author in quotation further expounds that prevention is at the core of contemporary notions of policing in democracy.

[889] BUSTOS RAMÍREZ, J. "Las funciones de la policía y la libertad y seguridad de los ciudadanos...", cit., p. 167. This preventive function, in the opinion of the author, is worse than repressive. He goes on to point out that prevention would be reduced to a feeling of security for part of the population.

community[890]. This situation is not exclusive to authoritarian regimes, although in these the risks are greater.

The power of secret surveillance is considered by the ECHR to be typical of the police state. In the *Case Klass and others v. Germany*, it finds it intolerable under the Convention, except insofar as it is strictly necessary to safeguard democratic institutions (para. 42), since society is currently threatened by very complex forms of espionage and terrorism, the State must be able to combat it effectively, through secret surveillance of subversive elements operating on its territory[891].

Today, technological tools play a very important role in this regard, as the police use them for a wide variety of purposes, ranging from deterring or intercepting crime to repressing protests and collecting data for future investigations[892]. In the opinion of JAR COUSELO, they are a double-edged sword, since they can lead to a drift towards a police state, with the risk of society being completely administered and directed by them, which could lead to a kind of "cybernetic totalitarianism"[893]. Therefore, in order to avoid such a situation, caution must be exercised and the use of the latter should not be extended to all cases, but only when required.

The police act in specific situations and towards specific subjects[894], so its role would be limited in this sense. However, it can also resort to surveillance instruments for the maintenance of security, which, in its various forms, is the preferred institutional response to address social problems[895]. Although these two concepts –surveillance and security– appear to be quite closely linked for some time now, they are distinct and each must be considered as a social process with its own dynamics and characteristic elements. Although they are connected, since the former is to be seen as the key to providing security at many levels, they have important differences. On the one hand, security refers to a goal, the pursuit of an objective, while surveillance is a practice, method or meaning. In this sense, the latter is often used as a means to a security end. Likewise, the latter often requires the former but there are other ways in which it can be achieved. Surveillance is sometimes carried out to provide or procure security, but there are additional purposes

[890] MARTÍN FERNÁNDEZ, M. "Policía, profesión y organización...", cit., p. 208; CRAWSHAW, R. "Introduction to the seminar on human rights and the police...", cit., p. 15. For the latter, the "order" guaranteed by the abuse of power is the ultimate disorder and the complete negation of the notion of law enforcement. Social order depends not only on policing, but on the exercise of good governance, especially in terms of social justice.

[891] RENUCCI, J.F. "Surveillance de masse et Convention Européenne des Droits de l'Homme", *Recueil Dalloz*, no. 3, 2019, p. 151. Following what is established by the indicated pronouncement, the author understands that this surveillance may only be deployed when it is a measure strictly necessary in a democratic society for national security and/or the defence of order and the prevention of crime.

[892] SLOBOGIN, C. & BRAYNE, S. "Surveillance technologies and Constitutional Law", *Annual Review of Criminology*, vol. 6, 2023, p. 220.

[893] JAR COUSELO, G. "El papel de la Policía en una sociedad democrática...", cit., p. 211.

[894] BUSTOS RAMÍREZ, J. "The functions of the police and the freedom and security of citizens...", cit., p. 171.

[895] HAGGERTY, K.D. "Surveillance, crime and the police", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 235.

for which it can be applied[896]. For all these reasons, security cannot be confused with surveillance. The latter, as we have said, is a means to achieve the former, but it is not the only one, and there are many others that have a lesser impact on the exercise of rights. Moreover, there are different forms of surveillance that can be more or less intrusive.

The task of choosing, within the legal limits, among the different existing mechanisms to maintain security, is the power of police officers, who have a wide margin of discretion to decide to adopt the measure or measures deemed appropriate and adequate for the prosecution and prevention of crimes[897], which may even differ in similar cases[898]. Thus, they have the ability to decide whether or not to resort to the FRs in the specific case, which we understand results in the reduction of the element of foreseeability which, as we have had occasion to indicate, is important when assessing whether the implementation of an instrument is adequate and does not exceed the limits in relation to rights, especially when the actions are carried out without the knowledge of the individuals involved in order not to hinder police work.

One consequence of leaving a wide margin of discretion to the agents is the arbitrary exercise of their functions. What happens with these mechanisms, especially with those that work in deferred, is that there may be an extension of the times and people under surveillance for the maintenance of security. This statement is due to the fact that their implementation in public spaces allows the capture of an indeterminate number of individuals –which can reach hundreds or thousands– who appear as potential suspects before the mechanism, with greater repercussions in the event that they are recognized by it and, even more so, when the results are erroneous. In addition, its retrospective use exceeds the temporal limits of its deployment for specific cases.

On the issue of discretion and arbitrariness of police use of FRs, the appellant case *R Bridges v. CCSWP and SSHD*, in which the Court of Appeal considers that a wide decision space is left to the police in the use of this instrument because it is not adequately regulated. This is because the regulatory framework is silent on the limits of certain fundamental issues such as where they can be implemented and the individuals to be included in the watchlist, i.e., who is subject to search[899]. However, the same Court left open the door to the possibility that an internal police policy document could comply with the law for the purposes of art. 8 of the Convention if it limited the discretion of individual

[896] LYON, D. & WOOD, D.M. "Security, surveillance, and sociological analysis...", cit., pp. 321-322.

[897] DUFFY, P. "Case-law under the European Convention of Human Rights relevant to the police", in *Human Rights and the Police. Seminar proceedings, Strasbourg 6-8 December, 1995*, Council of Europe Publishing, 1997, pp. 22, 23-24. See, in this sense, paragraph 90 of the ECHR judgement, *Case Murray v. The United Kingdom*. In it, the Court admits that law enforcement officers have a certain margin of appreciation when deciding both the measures to be adopted in general and in particular cases.

[898] JAR COUSELO, G. "El papel de la Policía en una sociedad democrática...", cit., p. 213. The author maintains that this has transcendental consequences.

[899] In the opinion of PURSHOUSE/CAMPBELL, if such criteria were included in the regulation, the requirement "in accordance with the law" would be satisfied. PURSHOUSE, J. & CAMPBELL, L. "Automated facial recognition and policing...", cit., p. 216.

officers, in the sense that it specified the subjects who may be on such lists and the locations at which FRs could be used. For that reason, South Wales Police could overcome this obstacle simply by making adjustments to its internal policy even though it lacked a positive legal basis for the use of such instruments. Moreover, it found that recourse to them was proportionate in the face of reasoned doubts about their operational utility and lingering concerns about the human rights implications of scanning hundreds of thousands of people to obtain comparatively few arrests[900].

For all these reasons, PURSHOUSE/CAMPBELL argue that the regulatory framework for police surveillance through FRs is based on a discourse of respect for human rights that serves to provide cover for the expansion in practice of generalized surveillance[901] . In this particular case, we have to take into account the particularities of the English system, in which what is not expressly prohibited is allowed. For that reason, capturing the image through FRs, as it is not prohibited by any rule, is allowed. However, the authors cited above consider that the freedom to implement mechanisms to fight crime does not extend to intrusive and open surveillance activities such as wiretapping and other interceptions of communication[902], reaching by extension to face recognition.

In this sense, in the case of taking and retaining photographs without automated processing, the situation is different because, although it does not have a solid legal basis, the common-law allows it and it would not be disproportionate because it does not run the risk of mass surveillance if they are only used in the specific case for investigative purposes. This situation can be seen in the ECHR *Case Murray v. The United Kingdom*. The ruling stems from the detention of Ms. Murray on suspicion of her involvement in terrorist activities. During the period of her detention, a photograph was taken of her without her knowledge or consent and linked to other personal and family data in a standard police database, known as a "pro forma screening". The domestic courts concluded that the taking and retention of photographs by the Army is a legitimate practice because, even without a specific legal basis, it is based on common law, as long as force is not used to obtain them and they are not used for defamatory purposes (para. 40). Similarly, the ECHR in para. 88 concludes that the measures adopted were in accordance with art. 8.2 of the Convention and, in para. 93 holds that the recording and retention of basic personal data cannot be considered to be outside the legitimate limits of terrorism investigation, which it extends to photographs.

However, as we have said, it must be taken into account that taking and retaining photographs in a specific case and directed towards a particular individual without the

[900] *Ibd*., p. 218.

[901] *Idem*. The authors adopt a critical position with the conclusions reached in this pronouncement. They argue on p. 211 that the legal basis for the surveillance exercised by the FRs is inadequate and that the legal framework that regulates the police use of this mechanism is too imprecise to protect citizens from abuse or arbitrariness. Such a normative framework and its interpretation in national courts transforms the protection of human rights into a box-ticking exercise, which excludes an important policy debate on the normative consequences of police surveillance through such instruments.

[902] *Ibd*., p. 219.

subsequent automated processing of biometric data is not the same as the implementation of FRs[903]. This is because the latter offer police forces enormous surveillance power, which is why we understand that all the circumstances and requirements that must be observed in order to be used must be delimited and expressly provided for by law, in order to prevent them from having a wide margin of discretion that allows them to freely decide when, where, how and to whom to direct the FRs, running the risk of deriving in a situation of absolute arbitrariness. As PURSHOUSE/CAMPBELL point out, the fact that only the collection of biometric parameters involving physical contact (such as DNA and fingerprints), or the practice of wiretapping on private property are considered truly intrusive practices, acts as a justification for allowing the police to use FRs without the authorization of the competent authority. Likewise, they have ample capacity to decide whether to implement these mechanisms[904], when in fact they should be subject to strict controls and restrictions.

Thus, biometric surveillance and, more specifically, through FRs, is presented to the courts as a police strategy aimed at ensuring high levels of security through effective control of crime, underestimating the strong impact it has on the freedom of the population and the consequent effective exercise of their rights. The damage at the social level is very high, which is why we believe that its use should not be extended, while at the same time limiting the ability of officers to implement them in the exercise of their functions of maintaining security, since, as DUFFY warns, it is very important to adopt effective and adequate safeguards against the abuse of police or security power[905], being necessary to carry out adequate controls on the discretion of the officers[906].

Despite what has just been pointed out, we must not forget that there are currently many conventional video surveillance and CCTV systems, which makes it very difficult for human operators to monitor all of them effectively, so that surveillance recordings are often used as passive records or evidence for investigations after the events[907]. In that

[903] PURSHUOUSE/CAMPBELL argue that LEAs have tended in recent times to make use of surveillance technologies in the performance of their basic duties, increasingly justifying their use by sensitivity to technological advances in the legal and technological fields. *Ibd.*, p. 220.

[904] *Idem.*

[905] DUFFY, P. "Case-law under the European Convention of Human Rights relevant to the police...", cit., p. 24.

[906] MURDOCH, J. "Police powers and criminal investigations...", cit., p. 127.

[907] GONG, S. et al. "Security and Surveillance", in Moeslund, T.B. et al. (Eds.), *Visual analysis of humans. Looking at people*, Springer, 2011, p. 456. The authors point out that incorrect detections or missed identifications can occur due to the limitations of single human control. They highlight four factors that may motivate this situation: a) excessive number of screens to monitor; b) boredom and fatigue due to prolonged monitoring; c) lack of a priori knowledge of the search target; and d) distraction caused by additional responsibilities such as administrative tasks. Similarly, the results of PIZA, E.L. et al. "CCTV surveillance for crime prevention...", cit. p. 149. In this study, the authors observed a significant reduction in crime when there was active CCTV monitoring while, on the contrary, when surveillance was passive, this did not occur. Therefore, they argue that such systems cannot act alone. One technique that could be implemented in this sense would be FRs, although there is no evidence on this.

This is not to say that passive systems are not useful, as they have proven their ability to generate forensic images, which can be used after an incident to identify suspects and details of the incident.

sense, FRs appear with the promise of speeding up this task, by providing greater speed and accuracy in the identification work, thus contributing to the improvement in security, at least in the feeling of it. However, these supposed benefits should not blind us and cause us to underestimate all the dangers they entail, legitimizing their use if we feel safer as a result.

III. DEBATE BETWEEN FREEDOM AND SECURITY

1. General aspects

Freedom is one of the most precious rights in a democratic State, since, through its guarantee, the exercise of other rights is allowed. In this sense, its deprivation constitutes the most radical form of state intervention[908]. On the other hand, security is also considered a right of citizenship[909] that the State and, by extension, the police, have the positive duty to actively protect, ensuring human rights, with crime control being the most common form of safeguarding them[910]. It goes far beyond protection against violence and the use of force, involving comprehensive protection of individuals against

SKOGAN, W.G. "The future of CCTV...", cit., p. 161. The author goes on to point out that using people to control the screens in order to quickly mobilize LEAs is more expensive than the passive mode.

[908] SAN MARTÍN CASTRO, C. "La privación de la libertad personal en el proceso penal y el Derecho Internacional de los Derechos Humanos", *Derecho y Sociedad*, nº. 20, 2003, p. 160.

[909] In this regard, among others, TAMBOU, O. "À la recherche d'un regime coherent de protection des données personnelles contre les mesures de surveillance étatique. CJEU, 16 July 2020, *Facebook Ireland and Schrems*, aff. C-311/18 (affaire dite *Schrems 2*) ; CJEU, 6 October 2020, *La Quadrature du Net*, joint cases C-511/18 and C-512/18 ; *Ordre des barreaux francophones et germanophones*, aff. C-520/18 ; CJUE, 6 octobre 2020, *Privacy International*, aff. C-623/17", *Annuaire Française de Droit International*, CNRS Éditions, Paris, 2020, p. 602 ; and BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública...", cit, pp. 253-254, 269. This position is not unanimous and some consider that security is not a right because, they argue, if it were so, it could become a "hyper-right" opposed to privacy and the protection of personal data and would result in a drastic limitation of freedom. This situation would occur because the right to security would imply an additional limitation, specific to all the others, beyond the general limitation of the exercise of the right by other individuals. See, for example, MITROU, L. et al. "Perceptions of videosurveillance in Greece...", cit., p. 130. The authors further argue that the invasion of the fundamental right to security would not solve security problems, but could be used as an argument to justify broader powers of state intervention.

[910] XENOS, D. "The protection against crime as a human right: positive obligations of the police", in Alleweldt & Fickenscher (Eds.), *The police and international human rights law*, Springer, 2018, p. 187. The author refers to this obligation of the police as a positive obligation, understanding as such those that determine the duty of professional care of the police and its officers. He points out that the duties of the former are described in terms of positive obligations of the State and are subject to certain conditions, finding their limits in negative obligations.

In this sense, we must state for the record that the term security for the purposes of our investigation is not linked to the right not to be arbitrarily detained, but to the state's duty to maintain social order and peace threatened by crime. In Spain there is no conceptual distinction, both being called security, while in France, for example, a distinction is made between "securité" and "sûreté". The former is linked to the aforementioned work of the State and its agents, while the latter is the individual's right not to suffer arbitrary deprivation of liberty. TERWANGNE, C. "L'illégalité nuancée de la surveillance numérique: La réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de Justice de l'Union Européenne", *Revue Trimestrielle des Droits de l'Homme*, nº. 129, 2022, p. 9.

threats. Therefore, it includes not only the assurance of the full and free exercise of the latter through the fight against crime, but also the requirement of an adequate environment for the development of peaceful coexistence, through the protection of the integrity of individuals, understood as the set of physical, psychological and moral conditions that allow their existence.

Thus, security is closely linked to freedom because the former appears as a necessary condition for the guarantee of the latter[911]. Therefore, as the Venice Commission points out, the maintenance of security –internal and external– is vital and essential for the protection of other essential values and interests, including democracy itself and human rights[912], which can only be exercised in conditions of freedom[913]. In a similar vein, BERNAL BALLESTEROS understands that security is the prelude to the enjoyment of all rights and, as a consequence, it reaches the dignity of persons[914] as a basic element at the apex of the system of rights.

As FERNÁNDEZ RODRÍGUEZ rightly points out, the relationship between both terms is complex, with multiple edges and aspects; and, in general terms, the union can be of two types: negative and positive. The first is based on an opposing dialectic, where the increase of one implies the decrease of the other[915], so that they are sometimes perceived as opposite values[916]. Along the same lines, it should be pointed out that, although the legitimate exercise of rights must be respected, as we had occasion to explain in the previous Chapter, it is not absolute and there are situations that justify its limitation, among which are serious threats to security. In this sense, rights can be evaluated and the restrictions placed on them must be justified. Likewise, security –at a given moment– may be above all others but, when making such a decision and adopting a measure restricting them, one must be aware that a right in question is being sacrificed[917]. It is therefore necessary to assess why the rights are important and whether they can be sacrificed for some other purpose.

In view of the link between both aspects, it is necessary to achieve an adequate balance between security and rights, and it must be assessed on a case-by-case basis, at

[911] GEARTY, C. "Escaping Hobbes: Liberty and security for our democratic (not anti-terrorist) age", in Reed, E.D. & Dumper, M. (Eds.), *Civil liberties, national security and prospects for consensus*, Cambridge University Press, Cambridge, 2014, p, 22.

[912] VENICE COMMISSION, *Report on the Democratic Oversight of the Security Services*. Study nº. 388/2006, Adopted at the 71st[st] Plenary Session (Venice, 1-2 June 2007). Strasbourg, 11 June 2007. CDL-AD(2007)016, pp. 4, 12, 13. Indeed, as the Commission makes clear, security is often proclaimed as the primary duty of the State.

[913] KATROUGALOS, for example, links security with autonomy and privacy. He argues that there is a need for protection of privacy in public space, even in places where one is visible to others. KATROUGALOS, G. "The tension between personal freedom and security from risks...", cit. p. 220.

[914] BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública...", cit., p. 269.

[915] FERNÁNDEZ, RODRÍGUEZ, J.J. "El encuentro entre seguridad y derechos humanos...", cit., p. 89.

[916] VENICE COMMISSION, *Report on the Democratic Oversight of the Security Services...*, cit., p. 13.

[917] HUGHES, K. "Mass surveillance and the European Court of Human Rights...", cit., p. 598.

the time of resolving the specific conflict, which has greater weight[918]. To this end, it will have to be taken into account that the limitation is equitable and respects certain express conditions that are appropriate for this purpose. Following on from what has already been stated in the previous chapter, in the part corresponding to the limits of rights, we can affirm that the State cannot restrict freedom beyond what is considered strictly necessary in a democratic society. Furthermore, this limitation must be legally provided for, and the rule that covers all aspects of it must be rational. In addition to the above, proportionality with its three variables must be observed.

The positive connection between security and rights or freedom to exercise them is complementary to the previous one. Under this latter perspective, it is considered that the greater the security, the greater the possibility of exercising them. On the contrary, a situation of greater insecurity hinders the application of rights, to the point of violating some as essential as life or physical integrity. In this sense, high levels of crime, including common crime, make it difficult for citizens to exercise the powers deriving from their rights[919]. The problem, as MURDOCH points out, is to determine how best to reconcile the exercise of police powers with individual freedom[920]. As noted above in the first section of this chapter, the public authorities have the obligation to maintain a high level of order so that life in society can develop peacefully. Thus, security appears as an essential public policy that must be implemented from the perspective of fundamental rights and, therefore, from the perspective of due process and judicial protection.

2. Need to find a right balance: special reference to the *Osman Test* and police knowledge of the existence of a security threat

The police have an obligation to act when there is a real and immediate risk of violation of rights through the commission of a crime. To this end, the Venice Commission considers it essential that the police be equipped with technological tools and have exceptional powers, although it goes on to point out that individuals must be protected against the abusive and illegitimate use of the information they have about them, since on many occasions, given the subjectivity and flexibility of the term security, together with its importance for the State, the latter has a wide margin of manoeuvre and may be tempted to use such instruments for illegitimate purposes[921]. For this reason,

[918] FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es)...*, cit., pp. 197-198. The author alludes to the fact that at a theoretical level the principle of proportionality is used, but its final solution will only come when faced with a real case. He goes on to argue that proportionality is the legal principle that must operate in the first instance when the legislator approves the regulations that allow the limitation of rights for security reasons and, in the second instance, must preside over the actions of those who apply the regulations.

[919] *Ibd.*, p. 199.

[920] MURDOCH, J. "Police powers and criminal investigations...", cit., p. 125.

[921] VENICE COMMISSION, *Report on the Democratic Oversight of the Security Services...*, cit., p. 4.

effective controls and a fair balance between freedom and security are needed, especially taking into account the information available to police services.

What has just been pointed out is the relevance of the latter when it comes to police action. There are three possibilities: a) the police know of the risk; b) the police should have known of the existence of the risk; and c) there is a real and immediate risk to human rights[922]. Thus, States must have some indication of criminality in order to collect and use data from individuals[923]. The ECHR has expressed itself on the issue of information and police action in the *Case Osman v. The United Kingdom*, establishing the so-called "Osman Test", by which the knowledge factor can be satisfied both in circumstances in which the police are expressly notified of the commission of a crime and when they should have knowledge of that risk if the circumstances of a particular case are similar to those of previous cases with the same characteristics. Thus, in the Court's opinion, when it is alleged that the authorities have violated this positive obligation, it must be shown that they knew or should have known at the time of the existence of the real and immediate threat to the rights of individuals and that they did not adopt the measures within the scope of their powers that, reasonably judged, could have been expected to avoid that risk[924].

Thus, the existing information on previous crimes and the foreseeability that similar incidents could occur at a given time and place, would be considered sufficient to establish the police duty to act in order to ensure crime prevention in specific situations such as violent sporting events, demonstrations and specific residential areas[925]. Likewise, the police duty to maintain security grows when the element of knowledge of the real and immediate risk of danger to it appears. This condition includes both the so-called "osman warning", where an express request for help has been made and from this derives the development of investigations in order to control the crime and protect the citizenry[926], as well as prior information from other similar incidents that make it reasonable to believe that a disturbance of security may take place. The more evidence there is, the greater the duties of the police to intervene, including additional investigations to apprehend suspects and protection from threats[927]. In this sense, taking into consideration that the existence of the latter, when real and imminent, is one of the exceptional circumstances for which the deployment of FRs is allowed, it could be thought that the police would be legitimized to trigger such mechanisms when they are

[922] XENOS, D. "The protection against crime as a human right...", cit., p. 199.

[923] VENICE COMMISSION, *Report on the Democratic Oversight of the Security Services...*, cit., p. 44.

[924] ECHR *Case Osman v. The United Kingdom*, 28 October 1998, no. 87/1997/871/1083, para. 116. The Court is aware of the difficulties of policing in modern societies, in view of the unpredictability of human conduct and the operational choices to be made in terms of priorities and resources. The obligation to protect security must be interpreted in a way that does not impose an impossible or disproportionate burden of crime prevention on the authorities. Accordingly, any risk to life may imply an obligation on the authorities to take measures to prevent that risk from materializing.

[925] XENOS, D. "The protection against crime as a human right...", cit., p. 200.

[926] *Ibd.*, p. 202.

[927] *Idem.*

aware that a disturbance of social order and peace may take place, based on the information available to them, either by having received a warning or by prior information.

Since police actions have an impact on human rights, the intervention must be carried out in terms of proportionality, limiting its exercise as little as possible. This assumes that the police do not go beyond and do not exceed their responsibilities, always within the framework of legality, in the exercise of their negative obligations, restricted by the rights of individuals[928]. Therefore, an adequate balance between the police functions of crime control and freedom is necessary. In this sense, the CJEU has positioned itself in several pronouncements in which it seeks to reconcile the requirements of human rights protection with those of security[929]. This balance will depend on the prevailing interest in each specific case.

As can be seen from all that has been said so far, freedom and security cannot be opposed to each other, since we are not dealing with two opposing concepts[930], but complementary ones[931]. Thus, the police cannot make disproportionate use of their functions in the maintenance of the latter, resorting to repression in such a way as to provoke fear, terror or intimidation in the citizenry, since such a situation also interferes with security[932]. As BUSTOS RAMÍREZ states, the relationship between the two concepts cannot be posed in terms of opposition, as one thing or the other, since they are not on equal terms and fundamental rights must have an absolute character in the State-citizenship relationship in a democratic system. There is no adjectival, conditional or circumstantial right to freedom or to life. It is not a question of deciding between one or the other, but of establishing perfect relations of subjection to the freedoms of the citizen with respect to state intervention. Security thus appears as a functional term, linked to each particular subject, with his freedoms, and which implies understanding the police to be at the service of society, which has to meet its protection needs[933].

---

[928] *Ibd.,* p. 209-210.

[929] This is the position of the CJEU in various pronouncements, in which it holds that Member States must respect strict proportionality for the implementation of measures facilitating mass surveillance, such as *La Quadrature du Net* (cited above); 16 October 2020, *Facebook Ireland and Schrems*, C-311/18; 6 October 2020, *Ordre des barreaux francophones et germanophones*, C-520/18.

[930] In this sense, BUSTOS RAMÍREZ understands both as specifications of the supreme value, freedom. BUSTOS RAMÍREZ, J. "Las funciones de la policía y la libertad y seguridad de los ciudadanos...", cit., p. 175.

[931] GEARTY, C. "Escaping Hobbes...", cit., p. 52; & HIRANANDANI, V. "Privacy and security in the digital age...", cit., p. 1101. The latter refers to privacy and security. However, as it links the former to freedom as a necessary condition for its exercise, we extend what it says to the relationship between freedom and security.

[932] BUSTOS RAMÍREZ, J. "Las funciones de la policía y la libertad y seguridad de los ciudadanos...", cit., p. 175. In the opinion of the author cited, what happens if the situation described above occurs is that the right to security is confused with citizen security as an instrumental or functional concept, from which the freedom-security contraposition is derived.

[933] BUSTOS RAMÍREZ, J. "The functions of the police and the freedom and security of citizens...", cit., pp. 175-176. Likewise, MITROU, L. et al. "Perceptions of videosurveillance in Greece...", cit., p. 134, when they state that Greek citizens consider that security and privacy are not mutually exclusive

However, in practice, at the individual level, citizens are willing to sacrifice part of their rights if this guarantees security, or at least a sense of it. On many occasions, it is not obvious that security expectations are consistent with what people are willing to pay[934]. On the other hand, it sometimes happens that the reactions and measures adopted against current threats are disproportionate and give excessive priority to security to the detriment of freedom. Thus, the discourse of human security has the capacity to inadvertently undermine the human rights regime[935] and cause citizens to expect very high benefits from police action in the area of security, making them unaware of the costs to their rights[936]. We believe that this unconsciousness has been fostered by the fact that the traditional human rights discourse has emphasized the nature of freedom as an individual right, while security is seen as a collective value[937], which must be protected against any threat in order to guarantee the correct exercise of that right and, therefore, life in society. However, as we have already pointed out, freedom must also be seen as a common, public and collective value[938] essential for a fair balance of the interests at stake.

The public authorities have the mission of guaranteeing a high level of order so that life in the community can develop in a situation of peace and tranquillity, intervening in it through policies that take into account the due respect and guarantee of the aforementioned rights. Citizens demand this action in different terms depending on the society and the moment in which we find ourselves, since the demand for security and the ways of guaranteeing it are a cultural issue[939] and depend very much on the public debate[940]. Despite this, what is common is the duty to reject disproportionate state

---

and expect the government to make an adequate balance and guarantee, through the adoption of measures, security and the enjoyment of civil liberties.

[934] STONE, C.A. & ZISSU, A. "Registered Traveler Program...", cit., p. 450. In the case of the RTP, society appears to be willing to be barred from taking a flight as part of aviation security or else pay the price of restricting rights by disclosing identity details and other personal information before arriving at the airport. All of these issues in the specific case are going to depend on elements such as the time available, the number of flights taken as normal or the experience of having been previously treated as a terrorist or not. The program is voluntary and individuals have the ability to voluntarily decide whether or not to enter the program.

[935] HOWARD-HASSMAN, R.E. "Human security: Undermining human rights?...", cit., p. 88.

[936] MARTÍN FERNÁNDEZ, M. "Policía, profesión y organización...", cit., p. 212.

[937] RUSINOVA, V. "Privacy and the legalisation of mass surveillance...", cit. p. 748.

[938] *Ibd.*, p. 749.

[939] In this regard, BUDAK, J. et al. "Citizens' privacy concerns. Does national culture matter?", in in in Friedewald, M. et al. (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, pp. 36-37; BAJC, V. "Sociological reflections on security through surveillance...", cit., p. 61, for his part, expounds that culture impacts security since it is influenced by cultural assumptions of what is considered an acceptable order of what is understood as disorder. It also impacts feelings about safety and potential disruptive forces. Past and present experiences shape feelings about safety and how the logic of safety translates those feelings into practice. FERNÁNDEZ RODRÍGUEZ argues that a more complex debate arises from the security-freedom debate, in which collective and individual interests are pitted against each other. Along with legal dialectics, sociological and philosophical elements are important. Culture influences legal dynamics and affects the decisions that are made. This situation has an impact on the field of rights, which are sometimes mediated by the cultural basis of society. FERNÁNEZ RODRÍGUEZ, J.J. "The encounter between security and human rights...", cit., pp. 91, 96.

[940] EIRENER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance...", cit., p. 3.

intervention in a democratic system[941], where the exercise of rights must be ensured as far as possible and can only be limited to the essential in order to provide high levels of security that facilitate, in turn, an adequate life in freedom.

Although the question of limits is complicated, two types can be distinguished: intrinsic or based on the conceptual contours of the right in question; and extrinsic. The latter would be the limits themselves, i.e., those created by the public power when the constitution empowers it to do so. These include the exercise of the right by others, the general interest or public order[942]. In the following, we will address the security argument as a justification for adopting measures restricting rights that may result in indiscriminate surveillance.

3. Maintaining security as argument for adopting generalized surveillance measures that restrict rights

The maintenance of security is one of the arguments put forward to implement certain rights-restricting tools, including those that may result in constant surveillance of the population. The AIA refers to this issue as one of the exceptional circumstances for using real-time FRs.

In a democratic society, it is generally accepted that there is a presumption against the monitoring of citizens. In this sense, the CJEU, at first, confirms the prohibition of generalized and undifferentiated surveillance measures involving the processing of EU citizens' personal data. However, it accepts them when the purpose is to address a serious threat to security and their implementation is for a specific duration[943]. In TAMBOU's opinion, the above immediately implies an acceptance within the EU of such mechanisms, so that it is understood that the end would justify the means to achieve it[944].

---

[941] However, it is difficult to strike a balance between the effectiveness of security and the preservation of the democratic system, because there is a risk of drifting into generalized surveillance. TERWANGNE, C. "L'illégalité nuancée de la surveillance numérique...," cit., p. 6.

[942] FERNÁNEZ RODRÍGUEZ, J.J. "El encuentro entre seguridad y derechos humanos...", cit., p. 92.

It is within the general interest and the maintenance of public order that security is found as a circumstance that allows the limitation of rights. Thus, by way of example, the articles of the Convention that list the rights that are endangered by the use of FRs in public places for law enforcement purposes, as we have already had occasion to explain in the previous chapter, establish public safety, the protection of public order and the rights and freedoms of others as situations that allow the exercise of each of them to be limited.

[943] It does so in various pronouncements issued in 2020. In this sense, see, TAMBOU, O. "À la recherche d'un regime coherent de protection des données personnelles contre les mesures de surveillance étatique...", cit. p. 595.

[944] This is because, although the deployment of such mechanisms is permitted within the EU, it does not extend outside the EU. Thus, for example, it is not permitted in the case of the USA, where it is considered that the standards of protection of rights are not as high as in the USA. *Idem.*

So, as we say, the implementation of a surveillance measure can take place. The forms in which this type of state intervention can be deployed are very varied, each requiring an examination tailored to the circumstances of the particular case. Generally speaking, however, for example, the use of CCTV in hotspots could meet the basic criteria (as set out above) if it meets certain conditions (i.e., if police access is only when a crime has been committed or if the movements of a person reasonably suspected of having committed a crime need to be monitored). However, there are some risks involved, such as the possible profiling of individuals, favoured by the use of FRs, since the latter allow risk management and the consequent monitoring of those individuals who are thought to be likely to commit a criminal offense because of the high risk of committing a crime[945]. In addition, it makes it easier for security guards to know at all times who is in a given place and, if combined with other types of biometric data, it is possible to obtain all the information on a given subject.

It is believed that through surveillance and early detection of problems, they can be solved quickly, thus guaranteeing security[946]. This leads to a disproportionate extension of the latter through surveillance techniques with perverse consequences on freedom. This is because preventive surveillance measures reach almost the entire population without limiting data collection to persons whose behaviour is likely to endanger public order[947]. Let us consider the case that, with the aim of preventing a serious threat to security, it is decided to resort to FRs in certain public spaces, using databases containing police images or images obtained covertly from social networks. In such a context, already the collection and maintenance of the data with which the tool works can cause this type of surveillance, to which is added the fact that it is capable of detecting and monitoring the movements of an undetermined number of people, affecting –among others– the right to privacy, the protection of personal data.

In this regard, we bring up the example of the FBI's "Next Generation Identification" program (using not only face biometrics, but also others such as iris, voice, etc.), which unifies databases in a centralized repository accessible to all government agencies. These data come from civilian, law enforcement and military institutions, to which are added photographs and other information provided by private entities such as social networks[948]. This combination of surveillance data and mass biometric identifiers

[945] MARCUS, S. & MILLER, S. *Biometric identification, law and ethics...*, cit., p. 35. The authors argue that if its deployment is finally consented, it should be subject to accountability mechanisms to avoid its misuse. The citizenry should be adequately informed about the systems and should have consented to their use for specific and justified purposes. Furthermore, it should have been subject to public debate.

[946] INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance...", p. 177.

[947] TAMBOU, O. "A la recherche d'un regime coherent de protection des données personnelles contre les mesures de surveillance étatique...", cit., p. 598.

[948] MILLER, K. "Total surveillance, Big data, and predictive crime technology...," cit., p. 111.

allows for "bureaucratized surveillance" which, as HU states, results in the mass tracking of ordinary citizens in forms of government that become commonplace and habitual[949].

The balance between security and rights is often characterized by the "trade-off" analogy, which, in HIRST's opinion, is not useful and creates a situation in which the maintenance and protection of one is at the detriment of the other. Thus, the more surveillance and the greater the infringement of rights, the greater the security protection. Mass surveillance has the power to infringe the rights of the majority, perhaps even entire populations[950], which can be achieved with the use of FRs.

Thus, after all that has been said so far, in our opinion, automated identification and social categorization systems have a direct impact on the pillars of democracy[951]. With the implementation of such mechanisms, there is a risk of normalizing the adoption of extraordinary measures that should be limited to exceptional circumstances, resulting in a type of routine surveillance. In the specific case of the "war of terror", as it is normally directed at individuals belonging to specific population groups, it interferes with their opportunities and life prospects[952], causing situations of discrimination, among other problems.

Despite the drawbacks, the CJEU accepts the deployment of surveillance measures for security reasons (the ECHR pronounces similarly in some judgements such as *Big Brother Watch*, as discussed in the previous chapter). It even values instruments that act in real time. In this case, it understands that they pose a serious threat to rights because they make it possible not only to locate individuals but also to have very precise information on their behaviour, which is why it only admits them with additional guarantees[953] . Thus, the State must demonstrate that the specific circumstances justify the existence of the threat and that it is real, current and foreseeable; the temporary

[949] HU, M. "Biometric ID cybersurveillance," *Indiana Law Journal*, vol. 88, no. 4, 2013, pp. 1478-1483. The author further notes that this process has been transformed with "cyberveillance" and "dataveillance". She thus speaks on pages 1480-1481 of the emergence of "bureaucratized cybersurveillance", through which individuals have normalized the use of cyber-surveillance techniques, since these are combined with traditional forms of registration and identity.

[950] HIRST, P. "Mass surveillance in the age of terror: Bulk powers in the Investigatory Powers Act 2016", *European Human Rights Law Review*, no. 4, 2019, p. 407. Thus, the author considers that putting national security and rights in a static position risks simplifying the complexity of the relationship between the two.

[951] Surveillance has led to the individualization of citizenship, which favours categorization and profiling. In this sense, individualization is the process by which a particular subject becomes part of a group of people and, in turn, that group is made up of subjects who can be governed. Once an individual is subjected to this process, it is possible to record information about him or her from birth to death. Classification makes the identification and consequent accumulation of information practical and workable. Raw information is not useful unless it is converted into data suitable for analysis, which means that the information has to be classified into categories. To this it should be added that classification also allows profiling, in the sense of establishing categories based on imagined characteristics of a social group as a whole. In the latter case, classification serves as an identifier of particular behaviours. BAJC, V. "Sociological reflections on security through surveillance...", cit., pp. 617-618.

[952] LYON, D. "Surveillance, security and social sorting", *International Criminal Justice Review*, vol. 17, no. 3, 2007, p. 162.

[953] See, C-511/18, para. 142-146.

limitation of the measure to what is strictly necessary for a period of time that must be established beforehand, although it is true that if the threat persists it can be renewed[954]. Similarly, in order to verify that the measure is not of a systematic nature, an effective control must be carried out before the independent authority; the algorithmic models used must be specific, reliable and non-discriminatory and subject to regular audits; a decision must not be taken based solely on the result of the instrument; the interested party's right to information when the investigation work is not compromised; and, in addition, the specific complementary guarantee of prior control by an independent authority or administrative entity is required[955]. Thus, in TAMBOU's opinion, the CJEU limits the possibility for States to adopt generalized and indiscriminate surveillance programs for security purposes[956] to compliance with the requirements and safeguards indicated, which coincide in part with what is established in the AIA.

For this reason, surveillance is not in itself a violation of rights[957], it will depend on the above as well as on whether it is the least harmful measure to achieve the intended purpose. However, in our opinion, tools that allow identification through FRs are still very harmful to fundamental rights and can lead to mass surveillance of citizens. Therefore, they cannot become a common and generalized instrument, as they are neither necessary nor proportional[958]. The threat to security is a powerful argument that can legitimize –under certain circumstances– their implementation, but, if so, all appropriate measures must be adopted to avoid their abusive use and, above all, they must be limited to a specific temporal, geographical and personal scope, and must cease to be used when the circumstances that led to their implementation have been extinguished.

Despite what we have just indicated, proponents of the technique claim great benefits in terms of security and threat prevention. Therefore, in the following, we will address the positive aspects of such mechanisms and whether they contribute as they claim to reduce crime rates and increase security, also favouring the identification of missing persons and victims.

[954] TAMBOU, O. "A la recherche d'un regime coherent de protection des données personnelles contre les mesures de surveillance étatique...", cit., p. 603.

[955] *Idem*.

[956] *Ibd.*, p. 604.

[957] YUDKIVSKA, G. "New approach to the right to privacy in times of transparency and mass surveillance...", cit., p. 57. The author argues that individual monitoring programs can be seen as necessary on their own, while when combined with others they represent a serious interference with rights.

[958] Similarly human rights groups argue that bulk powers are neither necessary nor proportionate, with the understanding that their interference with rights never will be. PRIVACY INTERNATIONAL, *Bulk powers in the investigatory powers bill: The question of trust remains unanswered*, 2016. Electronic resource obtained via the World Wide Web: https://www.politico.eu/wp-content/uploads/2016/09/PI_Lords.pdf, [retrieved on 2 September, 2024].

IV. SECURITY AN SAFETY BENEFITS PROVIDED BY FACIAL RECOGNITION SYSTEMS

The biometrics used at the 2001 Super Bowl may be arguably the most paradigmatic case of the deployment of FRs at mass events to maintain security in the U.S. in the aftermath of the 9/11 attacks that same year by recognizing the faces of suspected terrorists and dangerous criminals. As WOODWARD exposes, surveillance cameras surreptitiously scanned the faces of bystanders to capture images to which algorithms were applied to measure facial features, producing a "faceprint." The latter was instantly searched against a database of suspected terrorists and known criminals to recognize the targeted individuals[959]. Although considered a very useful tool for achieving the proposed security objectives, it did not produce any identification[960].

From what has just been explained, it can be easily concluded that, although the people who were not the object of the search went unnoticed by the system, they ran the risk of being detected by it, from the moment it scanned the faces of all those attending the event. Despite being a technique that, as discussed in the previous chapter, has important implications for citizens' rights and freedoms, it is no less true that it can also provide benefits in terms of security, being considered as an accurate tool to positively identify criminals[961]. This argument is used by those who defend the implementation of the instrument. Despite this, it should be noted that there are practically no empirical studies from the institutions that use them that offer data on this, which is why their real effectiveness in reducing crime rates has not been conclusively proven[962]. This issue is also lamented by SLOBOGIN/BRAYNE, who add that there are practically no studies on their empirical validity and effectiveness, arguing that most of the information on the effectiveness of the mechanisms is anecdotal and that academics and jurists depend to a large extent on the information issued by the companies that develop them, which may exaggerate their usefulness or underestimate the problems or disadvantages they pose[963].

There are studies that develop systems that can detect the face of known criminals, either in real time or delayed, from videos obtained from surveillance cameras that notify institutions once the match has occurred. In this regard, we bring up the one designed by KIM, et al. who suggest a high effectiveness of the tool they have developed for real-time detection of dangerous individuals in improving security, because it allows rapid

[959] WOODWARD, J.D. *Super Bowl surveillance....*, cit. p. 3.

[960] *Ibd.*, p. 9.

[961] GORDON, B.J. "Automated facial recognition in law enforcement: The Queen (on application of Edward Bridges) v The chief constable of South Wales Police", *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, vol. 24, no. 1, 2021, p. 3.

[962] CARVAJAL IBARRA, L.P. & ANDRADE ULLOA, D.L. "Impact of facial recognition technology on crime prevention," *Digital Anatomy*, vol. 7, no. 2.2, 2024, p. 217.

[963] SLOBOGIN, C. & BRAYNE, S. "Surveillance technologies and Constitutional Law...", cit., p. 220. On p. 223 of the same research, they point out that the Florida authorities consult the system 4,600 times a month but, of these consultations, only a small percentage allow opening investigations and, in California, the mechanism apparently resulted in one arrest in four years.

notifications to the authorities through the notification channel of the surveillance system[964]. However, even if the mechanisms to be implemented come with the promise of effectiveness in detecting criminals, there is still a lack of empirical data on their actual implication in lowering crime rates and preventing crime. Moreover, even in the case of CCTV, it has already become clear that it is difficult to know the real impact on crime reduction because it is impossible to know what the crime rate would be without cameras[965].

The only study we have found on the impact of FRs on crime rates is by WOODWARD, who reports that in Newham (England) the crime rate dropped after the police installed 300 surveillance cameras equipped with such devices[966]. The cited author believes that, although the technology has the potential to be misused in ways that undermine individual privacy, FRs have many positive uses, especially in terms of preventing terrorist and criminal acts at high-profile events, although he goes on to argue that criminals may only have moved on to other areas[967]. Therefore, even those in favour of the technique note some problems such as crime displacement, which is why we are sceptical about its implementation and the arguments used to justify it.

Thus, the only thing that is known is the effectiveness or accuracy of the mechanisms in the detection of faces at the time of their design and development and, subsequently, once implemented, the identifications in specific cases, as in the case described at the beginning of this section or in the *Bridges v. CCSWP and SSHD* ruling, in which the detection of one of the individuals being searched is described; or in more recent incidents, such as the assault on the Capitol on January 6, 2021. Through the "Faces of the Riot" app, the FBI was able to identify at least six thousand of the assailants. The app used 827 videos from the extremist network "Parler" where individuals shared videos and photos taken during the incident. From there the images of their faces were obtained[968]. In addition, at the international level INTERPOL makes use of FRs. it stores facial images from more than 179 countries, making it a unique global police database.

---

[964] KIM, H.B. et al. "Surveillance system for real-time high-precision recognition of criminal faces from wild videos" *IEEE Access*, vol. 11, 2023, pp. 56066-56082. Another system that acts similarly, in real-time, using CCTV data to identify criminals, is the one developed and presented in SANDHYA, S. et al. "Deep Learning based face detection and identification of criminal suspects", *Computers, Materials & Continua*, vol. 74, nº. 2, 2023, pp. 2331-2343. The latter aim to train the system to be able to identify individuals wearing masks or other objects that hide part of the face.

[965] HAGGERTY, K.D. "Surveillance, crime and the police...", cit., p. 241. There are some studies on the effectiveness of video surveillance cameras and computer vision but not on FRs in particular. See, for example, KIM, H.B. et al. "Surveillance system for real-time high-precision recognition of criminal faces from wild videos...", cit., pp. 56068-56069.

[966] WOODWARD, J.D. *Super Bowl surveillance....*, cit., pp. 9, 10.

[967] *Ibd.*, p. 12. He further argues that it can have benefits if used in the domestic sphere, for example, to ensure that minors on their way home from school are not pursued by pedophiles.

[968] BRACERO, F. "Una web facilita identificar a 6.000 de los asaltantes al Capitolio", *La Vanguardia*, 25 January 2021. Electronic resource obtained through the Web: https://www.lavanguardia.com/tecnologia/20210125/6196390/web-facilita-identificar-6-000-asaltantes-capitolio.html, [retrieved on 11 September 2024]. This application was later removed from Google and Amazon.

Since it was launched in 2016, it has identified nearly 1,500 terrorists, criminals, fugitives, persons of interest or missing persons, although it does not specify the numbers in each category or indicate how it contributes to security and threat prevention[969].

Despite the above, and in line with INTRONA/WOOD, many security analysts proclaim the efficiency and effectiveness of FRs, with the understanding that it is a neutral mechanism that offers the possibility of eliminating discrimination. The problem with such approaches is the way they frame the technology. They present it as neutral and non-problematic, when in fact –as has been discussed throughout our study– this is not the case and a more detailed and rigorous analysis of the benefits should be carried out. For example, in the case of terrorism, it could be argued that minor harms (such as biases and their consequent erroneous results) and loss of privacy is a small price to pay for security. However, the arguments presented are isolated and do not take into account all the ethical and legal issues behind the technology, but only claim the positive security effects. Moreover, they also often fail to take into account some fundamental technical issues involved in the effectiveness of the mechanisms, such as the quality of the images, the size of the database, the time elapsed between the collection of the first image to make the template and the capture of the subsequent image, etc.[970].

On the contrary, WOODWARD, advocating the implementation of FRs, puts forward a series of arguments to contrast some of the risks they pose, in line with many of the controversial aspects already discussed throughout this research. First, he argues that since the mechanisms act remotely, they are not physically invasive or intrusive and, for example, a metal detector is much more so. Thus, the author understands that the system helps to protect the privacy of individuals, although he points out –by way of criticism– that known offenders who are included in the database would have to face police scrutiny once they have been identified in a public place. However, he argues that these individuals already face scrutiny by the police, who already quite frequently resort to other biometrics such as fingerprinting[971]. As for the danger of incorrect detections, he emphasized that this risk is also present with traditional identification methods such as the comparison of mugshots. Moreover, the potential for error is reduced when matches from facial recognition have to be subsequently confirmed by LEAs. And, as the technique improves, failed identifications will become less and less common[972]. Despite what the author states, in our opinion, as indicated in previous sections, the deployment of FRs in uncontrolled spaces can lead to the incorrect identification of a very high percentage of individuals, even when the mechanism has a very low error rate, in addition to the problems related to the presumption of innocence.

Another of the arguments used by the author cited is the technological impartiality that offers benefits since it avoids human biases and preconceptions that can lead to racial

[969] INTERPOL, *Facial Recognition...*, cit.
[970] INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance...", cit., pp. 191.
[971] WOODWARD, J.D. *Super Bowl surveillance....*, cit., p. 11.
[972] *Idem*.

profiling. To this end, he argues that FRs do not focus on skin colour, hair style or manner of dress and do not have racial stereotypes. Therefore, he considers that the system acts objectively using mathematically measurable elements[973]. As already indicated, the instrument is not objective either and can reproduce existing prejudices in society, since it depends on the way in which it is trained, developed and used by the end users, as well as on the quality and variety of the information contained in the databases.

It also makes recommendations for the police, aiming to prevent abuses by FRs. In order to limit the function creep, he proposes to restrict and limit the information contained in the databases, which should contain only the necessary information and to specify who has access to it because very serious damage can be caused when they are accessed without authorization or the data is disclosed. Likewise, in order to avoid the excessive growth of databases and the joining of different ones, it is necessary to establish specific protocols to determine the information that can be stored, the time that can remain in the database and the conditions. In addition, it should specify the standards for considering the fundamental criteria for including someone on a watchlist, and unnecessary or incorrect information should be removed through periodic follow-ups. In order to prevent unauthorized disclosure of information, he considers it essential to establish strict controls, to which he adds the need to make the database secure and restrict access to it[974]. Finally, it states that the government should use the technology openly and provide as much information as possible to the public on the purposes and capabilities of the technique[975].

In view of all that has been mentioned throughout this section, we can conclude that the real benefit of these techniques in terms of preventing crime and maintaining security is unknown[976]. In the case of terrorism, attacks persist and the police continue to act after the fact. To give an example, although in this case there is no record of the deployment of FRs, last August 2024, a man of Syrian origin, belonging to the Islamic State, committed an attack in the German city of Solingen during the celebration of a festival commemorating the anniversary of the city that was estimated to bring together 800,000 visitors. With a knife, he indiscriminately attacked eleven people whom he attempted to stab in the neck. As a result, three were killed, five were left in serious condition and three others were slightly injured[977].

[973] *Ibd.*, pp. 11-12.

[974] *Ibd.*, p. 13.

[975] *Ibd.*, p. 14. In addition, it should collaborate with citizen institutions, such as oversight committees, which would be useful to ensure that abuses do not occur.

[976] As EIREINER states, "The safety benefit is hypothetical. EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance...", cit. p. 13.

[977] HERNANDEZ, J. "Lo que se sabe del atentado mortal en Solingen (Alemania) durante la celebración de un festival", *Huffpost*, 24 August 2024. Electronic resource obtained via the World Wide Web: https://www.huffingtonpost.es/global/lo-atentado-mortal-solingen-alemania-celebracion-festival.html, [retrieved 31 August 2024].

For this reason, we believe it is necessary to carry out studies to analyse the impact of FRs in reducing crime and preventing threats, as well as the negative aspects that their deployment may have on the rights and freedoms of citizens and their possible drift into a state of mass surveillance. For this reason, all aspects behind this mechanism must be considered before concluding its suitability. The main issue lies in how they spread and multiply, especially when it is a silent instrument that can reach ubiquity in a society increasingly dominated by new technologies, a feature that makes biometrics desirable for implementation in digital surveillance. This issue, due to its interest and relevance, will be dealt with in greater depth in the following section.

In this regard, we ask ourselves other related questions, since, for example, if terrorism is nowadays a diffuse threat and serious crime has a strong impact on society, should the movements of all possible suspects be monitored at any time and place, would it be sufficient justification to implement the mechanisms in public spaces in view of the fact that it constitutes a serious threat to security? The above scenario would imply a disproportionate use of the mechanisms and could lead to a state of constant surveillance similar to that of a dystopian society in which the digital panopticon would be the norm.

V. NEW TRENDS IN SOCIAL CONTROL AND SECURITY MAINTENANCE THROUGH DIGITAL SYSTEMS. ESPECIALLY FACIAL RECOGNITION

New technologies are involved in the transformation of contemporary society and have important consequences for social control[978]. Surveillance, as we have indicated, has become an everyday experience, despite the fact that it was traditionally associated with tyrannical states where it has been massively denounced[979]. This is a concept that, as with security, encompasses processes that include different and incomparable situations, which makes it difficult to elucidate and specify common patterns, classify phenomena and predict consequences. Today's surveillance has been enhanced and augmented by the use of digital tools, data and software[980]. All of these, acting together, are seen as powerful

[978] LYON, D. "An electronic panopticon? A sociological critique of surveillance theory", *The Sociological Review*, vol. 41, no. 4, 1993, p. 654.

[979] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*, Éditions Universitaires de Dijon, Collection Essais, Dijon, 2024, p. 8.

[980] As WANG/TUCKER state, "much surveillance is made possible by, and has in common, the technicalities of data and *software*". WANG, V. & TUCKER, J.V. "I am not a number': Conceptualising identity in digital surveillance", *Technology in Society*, vol. 67, 2021, p. 4. The authors develop an abstract framework that describes the essential components of surveillance and can be a research tool that encourages the sharing of methods and results. They divide the context of surveillance into four components: a) entity (people or objects exhibiting behaviour in space and time); b) entity behaviour observable through methods for creating and preserving behavioural data; c) attribute (behaviour observed by methods for specifying and testing specific properties of behavioural data; and d) identity (based on methods for assigning data to identities and naming them to distinguish them. They name data as identifiers for identities. Through these essential components of surveillance, they define surveillance as a process that

instruments for social control, especially dangerous and difficult to control when used by the police and the different agents of power, even in countries considered democratic, given that those in power are tempted to use them to exercise surveillance of the citizenry[981].

In the case of biometric identification, at a higher level of surveillance, making use of this data, individuals are classified into categories and influenced in their own opinions, opportunities, treatment and actions. Classification is now a form of identity construction in this new virtual social landscape. So identification is at the heart of all contemporary surveillance practices[982]. The fact that FRs are a discrete technology and operate at a distance –unlike others such as fingerprints or DNA– has favoured their use as a surveillance tool, as they act virtually unnoticed[983]. There is a risk that people's movements can be monitored and their images clandestinely captured; and, if the face data is linked to other databases that collect different parameters, a complete profile of individuals can be made, which can lead to "super surveillance"[984].

The fact that digital tools are available to the whole of society has favoured, apart from the generation of large amounts of data (with which the previous situation is enhanced), a new type of surveillance, in this case, horizontal, exercised among the citizens themselves[985], who control others through virtual interaction, especially through social networks. In this way, individuals adjust their behaviour –even their thoughts and opinions– according to the observation made of them by others[986]. Not only that, but also, at the vertical level, FRs favour social control[987]. The fact that they act silently and are embedded in CCTVs results in their flexible application that can take place at any time without the knowledge of the individuals[988], which can lead to the emergence of a feeling of constant vigilance derived from the uncertainty of not knowing when and how they can be used, thus enhancing an imperceptible social control over people, in the sense that

observes the behaviours of entities in a given context. Observations are made by testing the data offered by the context on chosen attributes, which provide a basic classification of the available data; they are chosen to detect only behaviours of interest that are specific to the data available in a context rather than to any intrinsic nature of the identity. They give two examples of context: 1) the activities of individuals when carrying their smartphones can be monitored; 2) smartphones can be used by users to spy on others.

[981] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*, cit., p. 8.

[982] WANG, V. & TUCKER, J.V. "I am not a number...", cit., p. 1.

[983] INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance...", cit., pp. 178.

[984] Thus, FRs can surreptitiously monitor citizens without their knowledge or permission, and this information can be combined with other personal data of different types that favour a superior intrusion into people's private lives. WOODWARD, J.D. *Super Bowl surveillance....*, cit., pp. 7-8.

[985] Currently, a type of surveillance is being enhanced in the criminal justice system, in which citizens are expected to inform police officers of the suspicious behaviour of others, being the "eyes and ears" of the latter, exercising surveillance through social networks and other similar tools of social interaction. LYON, D. et al. "Introducing surveillance studies", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 2.

[986] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*..., cit., pp. 74-75. The author describes this type of surveillance as excessive.

[987] INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance...", cit., pp. 178.

[988] *Ibd.*, p. 183, 184. The authors point out that the silent nature of FRs makes it difficult for society to scrutinize them. This situation creates a great opportunity for their pervasive use since the obscurity with which the mechanisms operate means that the population does not understand the risks involved.

they will adapt their behaviour to what is considered appropriate if they believe they are being observed, thus producing a sort of digital panopticon that could have an impact on crime prevention.

1. The "Banality of goods" used to guarantee security

A banal good is a mundane, commonplace object. The term "humility of things" is also used as a concept to express the way in which objects work invisibly and in a familiar, everyday way. This situation is particularly interesting in the field of security, where the instruments used for its maintenance are no longer perceived by the population. At first, the mechanisms are not considered habitual, but unusual, innovative, exciting or even worrying. Banality, therefore, is a process of formation of the meaning of the instruments that follows different evolutions and equally reaches different results in contexts that are also unequal. In that sense, CCTVs, despite being an image of totalitarian society[989], have become banal tools[990] because, in addition to being widely supported, they go unnoticed to our eyes and, therefore, we are not aware that we are being watched by video recording everything that happens in the place where they are deployed.

This is the case with biometric technologies, which at first seemed exotic, but their use has spread to the point of becoming commonplace[991]. Along these lines, in 2001, *MIT Technology Review* presented biometrics as one of the ten emerging technologies that would change the world and, indeed, this has happened. At that time, the population was reluctant to adopt them, but with the inclusion of such methods in conventional devices such as smartphones, this changed and their development and extension was accepted, showing them to society as everyday and innocuous tools[992]. In the case of FRs in terms of security, their increasing use by LEAs may cause some concern because all the

[989] HAGGERTY, K.D. "Surveillance, crime and the police...", cit., p. 241.

[990] GOOLD, B. et al. "The banality of security...", cit., pp. 978-979. The authors extensively study the banality of the objects used in the field of security through the analysis of CCTV in England. The same authors on p. 983 of this research, expose as one of the causes that have favoured the normalization of CCTV, the fact that everyday electronic devices such as Smartphones and computers come equipped with cameras and that these can be shared through social networks. This situation has caused individuals to become even more familiar with recording systems and they are not seen as problematic. We are in a cultural context in which people consider themselves "like a camera," which is why it is more difficult for those who are uncomfortable with surveillance cameras to determine exactly what would change if CCTV were reduced or eliminated. Thus, the authors themselves argue, there are cultural, political and crime prevention reasons behind why surveillance cameras have gone from novelty to ubiquity.

On the normalization and everydayness of CCTV, also MITROU, L. et al. "Perceptions of videosurveillance in Greece", in Friedewald, M. et al. (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, p. 123. In this case, as a surveillance mechanism used in Greece.

[991] WOODWARD, J.D. *Super Bowl surveillance...*, cit., p. 4. They are widely used in the private sector, both in commercial and civil applications, as well as in identity management in social networks and electronic devices. NORTH-SAMARDZIC, A. "Biometric technology and ethics...", cit. p. 433.

[992] ATICK, J. "Biometrics. 10 Breakthrough technologies 2001," *MIT Technology Review*, 2001. Electronic resource obtained via the Web: https://www.technologyreview.com/10-breakthrough-technologies/2001/, [retrieved on August 21, 2024].

problems that may arise from them are still unknown, although, if they come with the guarantee of offering greater security, perhaps they are viewed with hope, as a panacea to solve the current concerns that affect[993] . Although it is true that, once its use becomes generalized, it may become a banal good and, therefore, invisible, everyday, as if it had always existed, even more so when it acts remotely, goes unnoticed and is inserted in the already common CCTVs.

In this regard, it should be noted that camera surveillance is seen as an integral part of the infrastructure of public life and, in so doing, may have contributed to the creation of a new morality of personal relations in public. The latter, according to GOOLD et al., depend on the "comfort blanket" in terms of security, which is understood to be guaranteed by CCTV, thus contributing to an increased sense of security[994]. Not only have the instruments become trivialized, but so has security, as it has become part of everyday life and one of its most trivial aspects[995], with an almost unthinking acceptance of the need to protect oneself. Along the same lines, surveillance is allowed to extend to places and forms likely to undermine citizen guarantees and even endanger security itself[996].

Although the ECHR is concerned about mass surveillance methods, in specific situations such as the fight against terrorism, it considers that the trivialization of such methods cannot be discussed[997]. Also, as mass surveillance is used to prevent and act against the terrorist threat, it is fast becoming a new normal[998]. However, being a diffuse threat, as we discussed above, it may not be as effective as it is considered to be given that terrorist attacks continue to occur.

The problem here lies in the fact that, as soon as the measures go unnoticed by the population, there is no reflection on the issues that revolve around them. If security mechanisms are trivialized, they are left out of any inspection, reflection, dispute and debate, thus impacting on the quality and scope of democratic governance[999]. For this reason, we believe that it is essential that the instruments that enable this type of surveillance be subject to enhanced scrutiny and control, as well as to critical reflection before they are implemented and even once they are in use, otherwise there is a risk of their everyday use leading to their generalized acceptance.

---

[993] This situation already occurred with CCTV and its rapid expansion and standardization in England in the mid-1980s, to which also contributed the publicity made by the Government, in which these instruments were seen as suitable for fighting crime and the absence of a regulatory framework to regulate such mechanisms. What was developed were codes of good practice and guidelines for operators, but no substantive restrictions. GOOLD, B. et al. "The banality of security...", cit., pp. 980-981.

[994] *Ibd.,* p. 987.

[995] JENKINS, R. "Identity, surveillance and modernity...", cit. p. 165.

[996] GOOLD, B. et al. "The banality of security...", cit., p. 987.

[997] RENUCCI, J.F. "Surveillance de masse et Convention Européenne des Droits de l'Homme...," cit., p. 156.

[998] For this opinion, seeRUSINOVA, V. "Privacy and the legalisation of mass surveillance...", cit., p. 741.

[999] GOOLD, B. et al. "The banality of security...", cit. p. 993.

2. Digital panopticon

2.1.General approach to the panoptic theory

Modern society, especially in large urban areas, is characterized by invisible surveillance. Today, there is no need for a large number of police patrols in the streets because they are controlled by other instruments and technologies. In this sense, surveillance is becoming increasingly impersonal, general, without a specific target, whereas in the past it was usually directed at specific individuals. We are thus facing a situation in which citizens are tacitly and implicitly monitored, where the idea of the panopticon is seen as the archetype, if not the prototype of surveillance[1000]. Foucault's idea can easily be transposed to the present moment, where new digital mechanisms are increasingly being used to keep crime under control by monitoring and controlling the population.

Let us see briefly, in broad outline, what the author's general idea was –since it is not our task to delve into all aspects of his theory, because this task is far beyond our object of study– and why we find ourselves at this point.

The author proposes a disciplinary society, understanding discipline as the set of techniques through which the body can be controlled by means of coercion and management of individual movements in a given space and time. Thus, discipline is the method that makes it possible to control populations. This last idea is linked to the modern state, in the sense that it aims to carry out a massive control of individuals and their movements. It understands vigilance and constant observation as two key elements of power. With its exercise, it interferes in the decisions and movements of others. Now, power as a form of control is not based on physical force, but on knowledge. This means that it is based on the supervision and organization of individuals through strict technical methods. For this to be effective, knowledge is needed through which a classification of individuals is made. Thus, the body is not directly affected through physical punishment, but is organized, regulated and supervised[1001] by the powers of social control.

To devise his theory, he based it on Bentham's idea of the panopticon, although with some nuances, since the latter linked it to a prison system in which any movement of the inmates could be observed by the watchman from a watchtower located in the centre. The design was that of a semi-circular establishment in which the cells were arranged around it and control was maintained by the feeling of permanent surveillance[1002], although the guard was not in control of the inmates at all times, who could not see the guards and, therefore, did not know who wielded this power or when

[1000] JENKINS, R. "Identity, surveillance and modernity...", cit., pp. 162-165.
[1001] FOUCAULT, M. *Discipline and punish*, A. Sheridan, Tr. Gallimard, Paris, 1975, pp. 1-26.
[1002] LYON, D. "An electronic panopticon?...", cit., pp. 655-656.

they exercised it. It is therefore a device that rationalizes observation and surveillance[1003]. Thus, Foucault uses the panopticon as a metaphor to define the modern, surveilled society, in which efficient supervision and control of the citizenry is carried out. In the present, the panopticon escapes from the prison and is integrated into the city, where strategies of power and knowledge operate not only for criminals but for the population as a whole. Continuing with the metaphor of the panopticon, in the case of digital surveillance, LYON observes society as a prison, where invisible observers track the digital footprints of individuals[1004]. These observers would be the algorithms that take over the task of data analysis and interpretation that was previously the task of humans[1005].

2.2.The role of new technologies in the spread of the digital panopticon

The simple collection of personal data relating to criminal offenses committed by individuals, without major technological implications, is considered as a form of panopticon, since it allows the control and monitoring of the behaviour of individuals, not only in the field of crime, but also in other activities such as commercial ones. In this sense, GORDON in 1987 explained how the crime control function in the United States, after the implementation of the national computerized information gathering system, consisting of the creation of interconnected databases among different police forces, resulted in a "panoptic schema"[1006]. Similarly, COLACURI also alludes to the digital panopticon as a control system that would act as a kind of collective "super-ego" to remotely condition the behaviour of citizens and direct them to its monetization. There is also talk of a "Big brother" to describe the society endowed with mass surveillance of its citizens[1007].

Thus, the panopticon permeated society in general, as it went beyond crime prevention and reached broader political priorities. This was because information as power was used by the state to control the behaviour of individuals[1008]. He further noted that the system of information collection contributed to the rationalization of punishment and the reduction of its harshness and visibility, making it more widespread[1009].

[1003] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*..., cit. p. 14.

[1004] LYON, D. "An electronic panopticon?...", cit., p. 665.

[1005] EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance...", cit., pp. 8-9. The author goes on to indicate that this new observer is characterized by subtle interfaces and "black box" algorithms. Those who come into contact with the system are unable to understand it. A sense of mystification and alienation is produced.

[1006] GORDON, D.R. "The electronic panopticon: A case study of the development of the National Criminal Records System," *Politics and Society*, vol. 15, no. 4, 1987, pp. 487, 496.

[1007] COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali...", cit., pp. 124-125.

[1008] GORDON, D.R. "The electronic panopticon...", cit., p. 496.

[1009] *Ibd.*, p. 498. The author also points out that, although social concern about street crime legitimized the adoption of more efficient measures to control it, this does not explain the development of uncontrolled data surveillance.

If this was already happening almost four decades ago, the situation is aggravated by the introduction of powerful technological mechanisms capable of processing huge amounts of data in a very short time, as well as others that facilitate covert and massive observation in public spaces such as CCTV, and even more so those that use automated processing of facial images to identify individuals by comparing them with faces collected in databases.

2.2.1. Change of direction: from a disciplinary society to a control society

The model of the disciplinary society mutated over time, especially after World War II, to that of the "society of control". In the latter, DELEUZE observes control as the new monster of our time that replaces the traditional forms of discipline, appearing innovative mechanisms to exercise it, new weapons. While in the previous plane the watchman was very important, in the emerging one the code predominates as a password, that is to say, a numerical language of control composed of codes that allow access or not to information[1010]. Thus, the processing of the latter is the essential characteristic of such a society. The Internet and the diffusion of ICTS[1011] that allow the interaction of individuals on the digital world contribute to this situation, facilitating the loss of the physical and spatial characteristics of the panopticon, so that surveillance becomes just another part of the network infrastructure[1012].

In this new model, even the conception of identity is altered since, in order to interact in the virtual world, each subject has to provide data, personal or otherwise. Today, we are (re)known by codes, since all aspects of contemporary life are generated and encoded in binary numbers[1013]. As the interaction of individuals is increasingly digital, more data is generated in this environment[1014]. In addition, digital traces are left behind, i.e., information that allows predicting and regulating behaviour, being practically impossible to avoid being captured by the devices that perform monitoring[1015], while the digital traces of our activities and movements are a very useful type of information because they are revealing, cheap and easy to process, allowing the creation of a complete electronic profile of each person[1016]. Thus, the electronic devices used on a daily basis

[1010] DELEUZE, G. "Postscript on the societies of control", *Surveillance, crime and social control*, Routledge, 2017, pp. 35-37.

[1011] MATZNER, T. "Opening black boxes is not enough: Data-based surveillance in *Discipline and Punish* and today", *Foucault Studies*, no. 23, 2017, p. 31.

[1012] EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance..."," cit., p. 11.

[1013] WANG, V. & TUCKER, J.V. "'I am not a number': Conceptualising identity in digital surveillance", *Technology in Society*, vol. 67, 2021, p. 1.

[1014] *Ibd.*, pp. 1-2.

[1015] MARTÍNEZ, D.E. "Beyond disciplinary enclosures: Management control in the society of control", *Critical Perspectives on Accounting*, vol. 22, 2011, pp. 202-208.

[1016] YUDKIVSKA, G. "New approach to the right to privacy in times of transparency and mass surveillance...," cit., p. 57.

allow software to continuously monitor the population, since they include tools that generate, store and process data on their own operation. In this sense, as WANG/TUCKER rightly point out, "all software systems have the potential to be used as tools for surveillance"[1017].

The collection, processing and creation of data is a central issue to contemporary surveillance. The objective of the latter is simply to classify these data and use them for different purposes, from commercial to security maintenance. Such is the importance of information and digital identity that there is talk of "dataveillance" and "digital persona", these two concepts being closely linked. The former refers to the systematic use of tools that use personal data in the investigation or monitoring of the actions or communications of one or more people, while the latter refers to a model of public personality of individuals based on the data they generate through their usual activities executed through electronic devices. Thus, identity is fundamental to citizens' control over the information they reveal about themselves in different situations[1018].

It is not only the content of communications that is subject to storage, processing and tracking, because it also extends to metadata and traffic and location information, including telephone number, time of sending messages or emails, IP addresses, etc. All this makes it possible to know who is using a device or browsing the network, how and with whom, to which is added the information on the location of the devices. All this together makes it possible to draw very precise conclusions about people's lives[1019]. Thus, anonymity is now severely compromised, it is practically non-existent. As YUDKIVSKA points out, wherever you go you are still living in the public eye of the whole world. Everything is open, transparent, everything is recorded and stored[1020].

From what has been exposed so far, it should be noted that the theoretical perspective offered by Deleuze provides today important orientations including strategies of digital control and exclusion, although the new devices have greatly changed the dynamics of power and control[1021].

[1017] WANG, V. & TUCKER, J.V. "I am not a number...", cit., p. 3. Such is the importance of technologies in information processing that MILLER speaks of the "technology of surveillance". MILLER, K. "Total surveillance, big data, an predictive crime surveillance...", cit., p. 115.

[1018] *Idem*. The authors argue, in this sense, that, today, personal identity is more artificial, varied and fluid. Its fragmentation is promoted by the involvement of individuals with a wide range of digital services that demand the creation of data on people and products. The technical role of identity in surveillance is therefore of particular importance.

[1019] TERWANGNE, C. "L'illégalité nuancée de la surveillance numérique...", cit., pp. 6-7.

[1020] YUDKIVSKA, G. "New approach to the right to privacy in times of transparency and mass surveillance...", cit., p. 49.

[1021] Along with the above, it also assumes the neoliberal imperative to adopt constantly changing rules and requirements of "machining coupling" as "dividuals" rather than individuals. SEECAMP, A. & SÖFFNER, J. "A Postscript to the 'Postscript on the societies of control'", *SubStance*, vol. 53, nº. 2, 2024, p. 75.

Thus, SEECAMP/SÖFFNER speak of a new change in society, sponsored by new technological advances, especially AI and predictive algorithms[1022]. The authors in question state that this situation cannot be described from the panopticon as an optical metaphor in the sense of observing through individuals or certain devices to direct the behaviour of others, but that it is now monitored through the collection of personal data that facilitate prediction, management and control over it. In this case, control is not exercised through discipline, but through prediction and with the conformity of the individuals on their own, since it is they themselves who provide, through the use of electronic devices and interaction with entities and with others, their personal information. In this line, the population is not disciplined by surveillance because they do not even know that they are being subjected to it, because it is executed from decentralized cybernetic governance, which facilitates the prediction, manipulation and control of behavioural patterns rather than conscious decision making and self-control[1023]. WANG/TUCKER argue that it is perfectly possible for the digital infrastructure of our society to evolve into a digital panopticon, where seamless surveillance is possible across many connected contexts. They stress that the latest software developments (IoT, autonomous machines, networked services, etc.) facilitate such a situation[1024]. Therefore, Smart cities or, rather, Smart societies, in our view, have replaced disciplinary and control observation, giving way to algorithmic observation that is introducing profound changes in society.

In the field that concerns us, i.e., crime, the idea that delinquency can be prevented rather than punished has been fostered especially with technology, which offers new potentials in this regard. With the expansion of video surveillance, FR, behavioural and emotional state recognition, a new panopticon has been created that distinguishes only between the innocent and the guilty. In this sense, CHAZAL argues that society as a whole is seen as a potential criminal, from the moment it is subjected to omnipresent surveillance. However, he observes that there is a paradox and, at the same time that we criticize, we demand it when we are involved in an unpleasant situation such as, for example, robberies in public transport. Therefore, the one who accuses us on a daily basis is the one who, in turn, protects us[1025]. So surveillance is no longer confined to a specific person or to a specific space and time in order to discipline an individual who has committed a crime, but has led to the control of entire populations, exceeding the aforementioned limits.

[1022] *Ibd.*, p. 76. These tools make it possible to quickly analyse the enormous volume of data in police archives, facilitating their automated management. CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*..., cit. p. 45.

[1023] The authors consider that power is not exercised over people who feel that they are being watched, but over users who do not feel that they are being monitored. This control may not even come from the central government, but from large companies and organizations, except in authoritarian systems such as China's Social Credict System. This type of control has been referred to by them as "black panopticon". *Ibd.*, pp. 76-78.

[1024] WANG, V. & TUCKER, J.V. "I am not a number...", cit., p. 7.

[1025] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*..., cit., pp. 55-56.

2.2.2. The panoptic in the age of algorithms: What is happening with facial recognition systems?

All governments have always tried, in one way or another, to monitor citizens, but it is true that this task has been perfected with technology. Already at the time when photography appeared in the forensic field, the surveillance work was facilitated and this, for CHAZAL, already evoked the panopticon because these images will define the person as a criminal and, in a way, excludes them from society acting as the prison walls, thus expanding the space of confinement because the control devices go beyond the prisons. This control is increased when other personal and vital information about the subject is added to the image, causing the subject to be considered a dangerous being and, therefore, a threat to the social order[1026].

As technologies have improved, surveillance has adapted to new developments. Thus, for example, surveillance towers have been replaced by CCTVs which, in turn, have been equipped with different mechanisms to capture images, sounds and, currently, to recognize faces through automated techniques. Such systems, in line with the Venice Commission, can lead to a situation of ubiquitous and massive surveillance, since these mechanisms may not be visible to the public and the identity of the controller is unknown, which dilutes the appreciation and awareness of the existence of controls[1027]. Similarly, KATROUGALOS, argues that they are a ubiquitous surveillance mechanism that favours the panopticon situation in that they make it possible to control an entire city. He goes on to point out that it does not constitute a mere limitation of privacy, because continuous and systematic monitoring is not a simple exception to freedom because it can get out of control and the risk it poses is uncertain[1028].

"To be watched" is today's social norm. We live immersed in the panopticon or, better said, in different panopticons. There is not just one but several, depending on the context, which is why the actors will also be diverse: government-citizen, company-consumer, employer-employee or citizen-citizen. They are not watertight compartments, since the various contemporary panopticons are increasingly interconnected and the boundaries between them are blurring in the so-called "surveillance assemblage". In this way, the subjects targeted for data collection, whether public or private, coincide[1029]. Such a situation seriously jeopardizes rights, especially privacy, and this should encourage state intervention to protect it, acting as a sort of "privacy warrior". However, this does not

[1026] *Ibd.*, pp. 25-40. In the author's opinion, the registration and storage of photographs of prisoners, when this technique began to be used in the judicial system to control recidivism, already implied a surveillance task close to the panopticon.

[1027] VENICE COMMISSION, *Opinion on video surveillance in public places by public authorities and the protection of human rights...*, cit., p. 6.

[1028] KATROUGALOS, G. "The tension between personal freedom and security from risks", *Annuaire International des Droits de l'Homme. Conflicts de Droits de l'Homme*, vol. 4, 2009, pp. 215-221.

[1029] RUSINOVA, V. "Privacy and the legislation of mass surveillance...", cit. p. 749.

occur and the retention of data of all users of electronic systems is not only permitted, but also encouraged by the State in the event of serious threats to security[1030].

In view of the enormous power that algorithms have, the police could delegate their power to them and, in an extreme scenario, make use of them, not to support their action, but could become it, exercising a totalitarian control typical of a dystopian society that favours power asymmetry and one part of the population is controlled by the other[1031]. This situation is fostered by surveillance systems complemented by biometric data processing, allowing the development of a more effective and efficient identification mechanism[1032]. Thus, one of the objectives of FRs is to modify the behaviour of individuals in order to reduce undesired behaviours[1033].

In such a line, we bring up the example of the pilot project developed in Germany during 2017, with which FR mechanisms were implemented in the CCTVs of some train stations in the country, which showed that algorithmic surveillance is connected to the network and is not limited to a certain space nor has organizational barriers, because the data are not generated and interpreted with precise limits. Every individual who passes through the space that is subject to measurement, even for a brief moment, is recorded in search of a match with the database[1034]. For this reason, GATES refers to the "panoptic sort"[1035], increased in his view by the growth of image databases and the development of digital visual image processing techniques. He specifically points out that, in the case of FRs, the aim is to convert images of the face into coded information and automatically connect those with other documentary information on individuals. Thus, it is able to more fully and effectively integrate visual and documentary surveillance modes[1036].

As a part of the body is used for identification and, consequently, surveillance in order to control and prevent crime, we can understand, following CORALLO, that we are in a situation that promotes "biopoliticized surveillance", understood as surveillance that takes the body and its movements as the focal point. It is configured as a political

---

[1030] *Ibd.*, p. 750.

[1031] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*..., cit., p. 11; & EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance...", cit., p. 10. In this sense, the latter author is concerned about the uncertainty of the future.

[1032] LECHNER, M. "Tecnologías aplicadas a la seguridad ciudadana...", cit., pp. 6, 7. The author highlights biometric technologies as the last link in the complementation of the identification and control system.

[1033] In this regard, EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance...", cit., p. 11. The Berlin-Südkreuz pilot project, whereby automated face detection mechanisms were installed in CCTV installed in train stations, pursued this aim. Similarly, VENICE COMMISSION, *Opinion on video surveillance in public places by public authorities and the protection of human rights*, cit., p. 7.

[1034] EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance...", cit. p. 12.

[1035] A term proposed by GANDY, who understands it as a form of "high-tech, cybernetic triage" that uses transaction-generated databases to classify individuals according to their presumed economic or political value. GANDY, O. *The panoptic sort: A political economy of personal information*, Oxford University Press, 2021, p. 15.

[1036] GATES, K. *Our biometric future...*, cit., p. 112.

technique for managing the population in order to reassure it in the current uncertain and complex contexts, where security is the priority. Along with the above, he goes on to point out that "biopower", as power over the life and body of the species, is not an exclusive competence of the State but can be exercised by any organization through the collection of information and data management processes and tools[1037].

There is thus a close relationship between four essential elements that facilitate the panopticon and biopower: body, space, power and knowledge. All of them are essential in terms of surveillance and maintenance of control, especially the first one, given that when the body becomes visible, surveillance agents aim to achieve the ultimate goal of making individuals internalize control[1038], through the feeling of surveillance. In this way, it appears as a tool to determine power relations, in which the individual is observed as something to be dominated and trained to be docile and subordinated. Therefore, power appears as a way of acting that influences the thinking and behaviour of others, controlling them. Knowledge is an essential element in this process of surveillance and control, as it allows understanding the body and its characteristics, favouring the exercise of power. Once knowledge is possessed, power is able to reach the body, which is the ultimate goal of control. Therefore, power and knowledge are mutually dependent, since one cannot exist without the other[1039].

Currently, given the mass of information available, risk analysis derived from security threats is performed through automated databases with sophisticated data processing software, through which knowledge is managed. Such algorithmic prediction of risk behaviours is based on preventive targeting of crime and all human behaviours that pose a risk. This situation, as CEYHAN states, has led to "silent surveillance", highlighting among the mechanisms that promote it, the CCTV[1040], adding the FRs that are inserted in them, as they are likely to promote it.

In this sense, automation is key and, for ELMER, only through power, through the internalization of a probable gaze, can the panopticon be transformed into a disciplinary society that displaces and elides the face of power[1041], since it is not known

[1037] CORALLO, M. "Electronic Monitoring as an electronic panopticon: A Foucauldian perspective", *Manchester Review of Law, Crime and Ethics*, vol. 10, 2021, pp. 111-115. The author synthesizes all of Foucault's work and considers that, in a cyclical way, power enables the collection of more knowledge and increased control over the body; similarly, CEYHAN, A. "Surveillance as biopower", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 38. The latter considers that a new form of management of individuals is emerging: a new electronic and digital biopower that is more open, flexible and embedded in domestic life as opposed to the classical biopower of previous centuries.

[1038] KOSKELA, H. "'You shouldn't wear that body'. The problematic of surveillance and gender", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 51.

[1039] CORALLO, M. "Electronic Monitoring as an electronic panopticon: A Foucauldian perspective...", cit. pp. 111-115.

[1040] CEYHAN, A. "Surveillance as biopower...", cit. p. 43.

[1041] ELMER, G. "Panoptic-discipline-control", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 28.

when and by whom it is exercised, and this uncertainty favours the control of the subjects[1042].

In the current digital world, technological surveillance is increasingly tolerated[1043]. We accept being watched almost unconsciously when we use our electronic devices in the private sphere. However, when we want to refuse the subjugation of this type of technology in the public sphere, it is practically impossible, because it has permeated the latter and, therefore, it is no longer an option. Along these lines, it is very difficult to know when one is being watched and, following Bentham's initial theory, this uncertainty makes it possible for individuals to adapt their behaviour. In this sense, the system acts even when there is no one watching, since the fact of general visibility (being observable rather than being seen) will be enough to produce effective social control[1044]. This situation, far from being disconcerting, departs from the public debate because algorithmic surveillance in this space benefits those who are observed, albeit hypothetically, in the sense that it favours the feeling of security, at the expense of anonymity and privacy.

Similarly, VERMEERSCH/DE PAUW observe that society tends to value the preservation of its security much more highly than other rights, which is why panoptic surveillance is justified and supported, under the pretext that if one has done nothing wrong, one has nothing to hide[1045]. The basic assumption of this model is that a degree of privacy intrusion is necessary to achieve an optimal level of security. Similarly, citizens accept this impact on their privacy to achieve security at different levels[1046].

In line with the securitization process in which we are immersed, the use of technological systems is presented as a prerequisite and a "weapon of choice" to manage emerging security threats. From this perspective, they can reinforce the security continuum that would be likely to lead to a privacy vacuum where one's anonymity

[1042] In this sense, BOGARD, W. "Simulation and post-panopticism", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 31. To formulate his theory, he follows Bentham's ideal prison model, in which the architecture itself represents the reality and truth of power, regardless of the presence of a human observer in the watchtower. Thus, no observer is needed for the machine to function. It is a coercive strategy.

[1043] CORALLO, M. "Electronic Monitoring as an electronic panopticon: A Foucauldian perspective...", cit. p. 118.

[1044] REIMAN, J.H. "Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, pp. 160-161. In this scenario, the panopticon appears as a new threat to privacy because of the way in which our publicly observable activities are extended in space and time. If we direct our direct privacy protection efforts to reinforcing traditional privacy aspects, the new forms may be forgotten, as is the case with the digital realm.

[1045] VERMEERSCH, H. & DE PAUW, E. "The acceptance of new security oriented technologies...", cit., p. 53. From their study they draw some interesting conclusions, such as that individuals who are informed about the nature of the technologies, consider the surveillance exercised through them important and necessary to maintain security. However, they are also concerned about the lack of control and information received.

[1046] STRAUß, S. "A game of hide-and-seek? Unscrambling the trade-off between privacy and security", in Friedewald, M. et al. (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, p. 255.

becomes a space where every personal detail is made available by technology[1047]. Therefore, we currently live in an environment of complete transparency where every aspect of individuals' lives is known and there is a risk that this information will be used for monitoring in this current digital panopticon.

Following CHAZAL, the system is constructed in such a way that whoever tries to escape from it by rejecting the use of ICTS or the Internet will be declared, in the author's own words, a "vagabond des temps nouveaux"[1048]. The digital society has caused transparency to become a kind of ideal or moral value, making it difficult to know what part of privacy remains of the traces we leave behind from Internet searches, cell phone geolocation and surveillance cameras installed in the street. In view of this panorama it is very complicated to have any secret space, having to accept life under constant surveillance[1049], ubiquitous.

This last notion refers to the perspective of a world in which it is increasingly difficult to escape from the technologies of data collection, storage and classification, even going so far as to speak of ubiquitous computing, which is presented as a projection onto the physical world of the capacity for networked interaction with which users can be known and their data recorded. In view of the above, ANDREJEVIC considers that this form of interaction is transferred to the urban environment and the question of anonymity in it, because spaces have been created that allow people to be recognized wherever they go and, from this, personal information is extracted and recorded, creating a completely monitored space, via the various surveillance technologies available[1050]. Not only that, but the author also alludes to models of overlapping surveillance enclosures, which more accurately describe a territory that is totally surveilled, a world characterized by the proliferation of surveillance networks with different capabilities for capturing information under the control of different entities, all of which transforms the experience of everyday life into a large laboratory[1051].

The panopticon derived from the FRs favours a generalized surveillance, both of criminals and of the general public, without knowing exactly when it is in operation[1052]. This situation is accepted by the common population under the argument that it allows for a higher level of security, at the expense of other rights. Therefore, in line with GATES, we are facing an urban dystopia, since the implementation of the latter creates a prison-like environment where the exercise of liberties by citizens is diminished from the

[1047] *Ibd.*, p. 259.

[1048] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*, cit., p. 8.

[1049] *Ibd.*, pp. 8-9. On p. 52 of the same research, the author alludes to subcutaneous chips as a possible surveillance tool that is not yet in use but which, he predicts, could spread and replace the identity card, posing, in his opinion, a danger to social order, since society would be controlled and strongly limited in its individual freedom.

[1050] ANDREJEVIC, M. "Ubiquitous surveillance", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, p. 92.

[1051] *Ibd.*, pp. 93, 96.

[1052] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique...*, cit. pp. 57-60.

moment they are under constant police observation[1053]. There is no way to escape surveillance unless, as CHAZAL states, we become aware of what limits us and act accordingly[1054]. We cannot close our eyes to reality, in the sense of thinking that this surveillance does not occur simply because we do not see the devices that execute it. We must not get trapped in the myth of the immateriality of digital technology and understand that, since it cannot be seen, it does not exist. On the contrary, we must become fully aware of its existence, of its ubiquitous and timeless action, in order to understand the risks we face.

[1053] GATES, K.A. *Our biometric future...*, cit., p. 94.
[1054] CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique...*, cit., p. 68.

CONCLUSIONS

CONCLUSIONS

FIRST. Biometric identification is not the same as emotion detection and biometric categorization.

When recognizing individuals, different parameters are used depending on the greater or lesser capacity for individualization. General indicators or "weak biometrics" are linked to the recognition of emotions or intentions and the categorization of people. Although they can be useful in police work to detect a crime before it takes place and thus prevent it, as is the case with the detection of intentions through changes in facial expression or suspicious movements, they differ from biometric identification. This is because the latter uses strong biometrics to determine the identity of the subject in question, while the former does not, although it is true that they can be used as a complement to the work of the latter. Therefore, biometric identification is not the same as emotion and biometric categorization.

SECOND. Biometric systems has two different functions: identification and verification.

Identification consists of the automated recognition of certain biometric characteristics, through their comparison with those of other individuals stored in reference databases and, in general, it is of the one-to-many type, and there may be no knowledge or consent of the identified individual in the processing of his personal data. Verification falls outside this category because it consists on the confirmation of the identity of a particular person by means of the data previously provided by the owner himself, with the existence of consent. For this reason it is one-to-one and is usually used to access certain places or devices. Along with the difference in terms of consent, another important distinction is the consideration of the personal data used in the former as particularly sensitive in the GDPR and LED. Moreover, as in our study they are linked to crime-related activities, the AIA understands them as sensitive operational data. To the above it should be added that the latter does not regulate verification systems because the impact on citizens' rights is not so high such as systems that perform the identification function. Therefore, biometric systems have two different functions with various implications.

THIRD. Modern facial recognition mechanisms use AI systems for identification.

RBIS, including FR, are AIs whose function is to identify individuals without their active participation and at a distance, by comparing the face data of an individual with those contained in a reference database. Normally, Deep learning techniques are used to perform this task, which is why we are dealing with artificial intelligence mechanisms trained to compare and identify images of faces through a complex mathematical process.

FOURTH. FRs in public places for law enforcement purposes have specific risks and need to be studied in depth.

The use of FRs has become widespread in a multitude of activities in both the public and private sectors. In the former, they can be used by LEAs to perform the function of law enforcement (preventing or controlling crime) in publicly accessible places. In the latter, the risks to the rights and freedoms of citizens are greater because an indeterminate number of individuals can enter the field of vision of the mechanism and provoke, in extreme cases, a state of mass surveillance. For this reason, given the dangers that may arise from their use, the systems that act in public places need to be studied in depth and independently from their deployment in other contexts such as border control, airports or critical infrastructures, as the latter are controlled environments with different characteristics comparing to the former.

FIFTH. The new crime scenario means that new prevention and control mechanisms must be sought.

Crime is changing and adapting to new technologies. Criminals use AIs as an instrument to commit crimes, not only traditional ones, but also other new forms of delinquency are appearing through the use of such systems. As a result, the current crime scenario creates the need to look for alternatives to conventional prevention and control systems, among which are FRs.

SIXTH. The use of RBIS, especially FRs by LEAs is becoming more and more frequent.

Since the first biometrics-based systems began to be used in the field of law enforcement, they have been evolving and adapting to new technological and social changes. In the case of FRs, their operability and easy insertion into conventional video surveillance and CCTV systems, which are becoming more and more frequent, has led LEAs to increasingly use such mechanisms, resulting in their widespread and common use in the field of law enforcement in public places.

SEVENTH. The AIA regulates the AIs with an approach based on the risk to fundamental rights.

The AIA is a novelty because it is the first normative text coming from a public institution that regulates AIs. It is developed with an anthropocentric rights-based approach. Thus, it classifies the mechanisms according to this criterion, establishing different requirements and guarantees depending on the consideration that each one has. Thus, it prohibits those that entail an unacceptable risk and establishes restrictive conditions for those of high risk, progressively reducing them to those that pose a minimum risk, which have no restrictions at all. Therefore, the AIA classifies AIs according to a risk-based approach to citizens' rights.

EIGHTH. The AIA distinguishes the RBIS used in the public area by LEAs for law enforcement purposes according to the time it takes to perform the identification, allowing the use of those that act in real time in specific situations.

The AIA is the regulatory framework of reference for the use of RBIS in the public domain for law enforcement purposes, at least for those acting in real time. However, for what is not covered therein, it will have to be governed by the GDPR and the LED. The latter, regulating the protection of personal data in the criminal field, is the legislation that applies to our study.

One of the novelties of the AIA is the distinction of the RBIS in the scope of law enforcement according to the time they take to perform the identification. It classifies them into those that act in real time and those that act in deferred time. The former it considers to be an intolerable risk and, therefore, their use is prohibited. On the other hand, the latter, having an impact on rights but not as intense as the former, are considered high risk, and must be subject to the measures and guarantees established in the AIA for the systems it considers as such. The situations in which RBIS can be used are three: targeted search for victims of a crime or missing persons; prevention of specific, significant and imminent threats to the life or physical safety of persons or threat of terrorist attack; and location or identification of perpetrators or suspects of a serious crime specified in Framework Decision 2002/584/JHA and punishable in the Member State by a sentence of at least four years. Thus, AIA allows the use of FRs in real time in specific situations.

NINTH. The situations in which real-time RBIS can be used allow for their broad use, from which some problems arise.

The exceptional circumstances in which the use of real-time RBIS is foreseen favour their wide use, which gives rise to some important controversies and consequences. On the one hand, the limitation in relation to the list established in the Framework Decision is insufficient because it is not restrictive enough, given that some of these offenses are not serious enough and may lead to excessive and unjustified recourse to these mechanisms. In order to be more limited, it should be completed with the inclusion of the reference to the profile of perpetrators, more restrictive, in the sense that they have to be "particularly suspected by the police". On the other hand, it is not clear what is to be understood by imminent threat to the life or safety of natural persons, leaving this task to the free decision of the agents in charge of its implementation, thus granting them a wide margin of discretion. However, it does specify that the deployment of the mechanisms must observe a series of requirements, among which is the performance of a rights impact assessment by the agent in charge of its use, also taking into account the circumstances in which it will be carried out, specifically those relating to the nature of the situation and the consequences derived, in addition to temporal, geographical and personal limitations.

The use of FRs by LEAs is subject to prior authorization by an independent administrative or judicial authority, which may refuse it if the use is not necessary and proportionate. However, the problem appears when, for reasons of urgency and necessity, this requirement can be saved and the agents have the capacity to implement the mechanisms, even in situations that do not require it, using such arguments. In this sense, prior authorization must be mandatory in all cases, otherwise the systems could be extended irrationally and severely impact the rights and freedoms of citizens. Even if the authorization is not initially requested, it must be asked for retrospectively within a maximum period of 24 hours. However, despite the short delay, the rights and freedoms of citizens have already been violated.

Another controversial aspect of the AIs as far as RBIS is concerned, is the provision that each Member State must expressly include in its domestic law whether they allow the police use of this measure, in what terms, under what circumstances and guarantees, although they must always be more restrictive than those established in the Regulation. This is because the EU continues to delegate competences in security matters to each country but, with this, there is a risk of regulatory fragmentation, since each State will be able to include such mechanisms in the form it considers most appropriate, which may differ considerably from one country to another.

Consequently, despite the apparent prohibition on the use of RBIS that act in real time and, by extension, of RFs, the AIA allows broad recourse to them, which gives rise to some serious problems, such as those mentioned above and others linked to the rights and guarantees of the population.

TENTH: Delayed RBIS are high risk systems. They must observe the guarantees and requirements foreseen in the AIA and are subject to the provisions of art. 10 LED, not as strict as those foreseen for those that act in real time.

Delayed RBIS, i.e., which operate over a longer period of time than the previous ones, also have an impact on citizens' rights and guarantees but, according to the AIA, with a lower intensity. Therefore, they are not prohibited but are considered high risk in the AIA given their capacity to interfere in those and the possible technical deficiencies susceptible of issuing biased results and causing discriminatory effects.

The requirements to be observed are based on proportionality and legitimacy, strict necessity and selective action in relation to the persons to be identified, location and temporal scope. In addition, the set of data used must be limited and obtained in a lawful manner. The requirement for authorization is also maintained, but in this case with a more extended period of time. In addition, the AIA prohibits its use in a way that leads to a situation of indiscriminate surveillance.

These systems are regulated by the provisions of the LED, which acts as *lex specialis* in this case. It prohibits the use of biometrics in its article 10 unless there is an essential public interest such as citizen security. Because of that, when the use is

authorized, the requirements to be observed are those commonly established in art. 4.1 of this regulation. Among others, the data must be processed in a lawful manner.

Thus, the requirements and provisions foreseen for this type of system are laxer than those for systems operating in real time, even though they can also identify thousands of people in a short time and have an intense impact on citizens' rights and freedoms.

ELEVENTH. All RBIS present serious risks to rights and freedoms, which is why they should be given identical consideration.

Both real-time and delayed systems have a serious impact on the rights and freedoms of the population. The level of such interference does not depend on the data processing time but on the volume of people likely to be subject to the measure and the consequences that derive from it. Moreover, with the latter, there is a risk of deriving in a scenario of indiscriminate surveillance if they are resorted to on a continuous basis. Therefore, the distinction made in the AIA based on the supposedly different level of impact is artificial and not in accordance with reality. Consequently, it is more appropriate to consider them identically, understanding that they both have a severe impact on the interests of citizens, and should be subject to the same requirements and restrictions.

TWELFTH: The ever-increasing volume of data and the existence of sophisticated mechanisms capable of processing it leads to a very dangerous situation of "dataveillance" and "algorithmic surveillance".

Data-based surveillance and algorithmic processing of data has a serious impact on citizens' guarantees. The people and institutions with the power and capacity to use them have an unimaginable power of surveillance and control, which runs the risk of leading to an authoritarian state in which restrictive decisions are taken that directly affect citizens, even restricting or limiting their movements. This is therefore a dangerous situation that must be avoided.

THIRTEENTH. The face and its image are especially sensitive private data.

The face and its image are elements that contain sensitive information exclusive to each person that allows his or her identification, and therefore require specific guarantees for their protection. This consideration also extends to biometric templates because they also allow the identification (in this case automated) and biometric comparison of individuals. Data processing is already an initial phase in the processing of such sensitive personal information. Its inclusion in a database causes the face to acquire such consideration, since biometric data are understood as such. So, the face, its image and biometric templates are particularly sensitive private data.

FOURTEENTH. The face is the same as other biometrics in terms of intrusiveness. Physical contact is not a determining factor to exclude it.

The face is different from other biometrics because the information from it is visible to the public and can be collected from a distance, not affecting bodily integrity

since no personal contact is required. However, it can be performed without the knowledge or consent of the data subject, which is why there are risks in relation to informed consent and privacy. Likewise, the data subject is exposed to a situation of defencelessness against those who use biometrics for surveillance purposes. For this reason, physical contact is neither a sufficient nor an adequate criterion to determine the degree of intrusiveness of a biometric instrument, and the use of the face for identification purposes is understood to be equally or more intrusive than other biometric parameters.

FIFTEENTH. FRs have an impact on individual and collective rights, as well as on human dignity.

FRs not only interfere with rights at the individual level in the private and social sphere of the person, since they also reach the collective level, being capable of affecting the political, social and democratic stability of a country. Therefore, they reach all levels and have serious results. As a consequence of the above, human dignity, as a pillar of the system of rights, is affected by FRs from the moment they interfere with them and individuals feel uncomfortable with surveillance through biometrics. Moreover, with their use, people are reduced to mere data, which results in their dehumanization or reification; and, at the collective level, they reach the political order and social peace. Thus, human dignity is seriously affected by the use of FRs and their impact on rights at all levels.

SIXTEENTH. Privacy is one of the rights most compromised by the use of FRs and its limitation has repercussions on the exercise of other rights.

Individuals have the right to keep certain aspects of their lives, including those involving interaction with others and public space, private. This is affected by the covert recording of images for police investigative purposes, even more so when FRs are used. Such mechanisms interfere with privacy in all the phases in which they operate, from obtaining to storing and using the information, insofar as they make it possible to link and connect face data with those contained in other databases. This is compounded by the use by others of information as sensitive as facial data is, which can even be collected on a massive and indiscriminate basis. Although there is less privacy in the public space, it is no less true that citizens have a reasonable expectation that they will not be subject to surveillance by large-scale data collection and processing tools such as FRs. Therefore, even in the public area, the right to privacy in terms of one's own information is still invoked.

As a matter of fact, privacy is one of the rights most affected by the use of FRs and chilling effects can result from this given the impact it has on other rights such as freedom of expression, peaceful assembly, association, etc. This situation occurs when individuals change or restrict their activities, especially in the public space, for fear of being subject to surveillance by such mechanisms and the repercussions that may arise, especially at the level of police investigation. On the other hand, the right to privacy acts

as a limit to the power of state surveillance, since a series of requirements and guarantees must be respected for the use of similar mechanisms in this case.

From all of the above, it can be concluded that privacy is greatly affected by the police use of FRs in the public sphere, being one of the most violated rights, which can result in the restriction of daily activities by citizens, reaching the exercise of other rights and freedoms. In this way, it is necessary to protect the anonymity and privacy of personal information.

SEVENTEENTH. The use of FRs makes greater protection of personal data necessary.

New technological advances that involve the use and creation of data lead to an increase in the massive electronic recording of such data, including biometric data. This creates a situation of electronic surveillance that generates the need to protect them in order to safeguard the citizenry itself. As in the case of privacy, FRs have an impact on the protection of personal data in the different moments in which they act, starting with the collection of information. To safeguard this right, various regulatory texts have been enacted to provide enhanced protection for personal data.

EIGHTEENTH. The sources from which information is obtained are diverse. In the case of social networks, as in the physical public sphere, there is an expectation of privacy in the digital space, not being able to obtain personal data from social networks regardless of their configuration.

The sources from which information can be obtained to use FRs can come from police databases as well as from individuals being pursued and, in that sense, there would not be many difficulties. However, when social networks are used, things change and problems arise, not only when the information is used to train the mechanism but when it can be included in databases used in the search for criminals and terrorists. Controversies increase when private companies, using "data scraping", collect this data massively and sell it to LEAs. Although this technique is used in some countries such as the USA, in the EU it is prohibited in data protection regulations, which is why it cannot be applied in the European Union.

Individuals are increasingly sharing personal content on social networks and other virtual areas, which may be public, or in other words, without access restrictions; or private, that is, limited to users who are connected to the account or profile in question. In the first case, it may seem that the fact that the user publishes images or videos makes the data manifestly public and, for this reason, he or she would be giving his or her consent (even if tacitly) to its processing by others. However, despite the possibility of access to the content by an indeterminate number of users, its disclosure or use by third parties is not accepted. Thus, as occurred with the right to privacy in the public sphere, there is an expectation of privacy on the part of social network users that their data will not be used for purposes other than viewing it or any other to which they have given their express

consent. What has just been pointed out extends to private accounts. As a result, personal data cannot be obtained from social networks, regardless of their configuration.

NINETEENTH. Consent is irrelevant and the right to information may be limited in the processing of personal data by RBIS in the police field.

Consent is the basis for the processing of personal data. For it to be valid, a series of requirements must be observed, such as the subject being duly informed. Despite its importance, in the police field it is irrelevant, as is made clear in the definition of RBIS established in the AIA. Irrelevance arises at least in relation to the subjects to whom the measure is directed, that is, terrorists and suspected criminals with the aim of not obstructing the investigation. On the other hand, another of the requirements (closely linked to the previous one) for an adequate use of the systems is the right to be informed, which can be expressly limited when the investigations are covert and video surveillance is used in the criminal field, and must meet a series of requirements, such as being a proportionate and necessary measure in a democratic society. Furthermore, to ensure proper use of the systems, the principles of transparency and public scrutiny must be respected. Therefore, consent is irrelevant and the right to information is very restricted in the field of police investigations regarding RBIS, at least as regards those who are the subject of the search in order not to hinder the investigation. However, the cause must be strongly justified and, in any case, basic information on the processing and use of the data must be provided.

TWENTIETH. Personal data may only be used for specific, explicit and legitimate purposes. For this reason, they must also be specified in the delayed FRs, which must be the same as those for which they act in real time.

The processing of personal data must be done for specific, explicit and legitimate purposes, including the maintenance of security and the prevention of crime and public disorder, as well as the protection of the rights and freedoms of others. In this sense, the use of FRs by LEAs in the public domain for the purposes of compliance with the Law in real time would be permitted in these cases, as the exceptions provided for in the AIA coincide with those mentioned. However, it cannot be extended in all cases, since, for it to be lawful, a series of requirements must be observed, such as the fact that the crime must be serious, and it cannot be extended to other illegal acts and situations that do not have such consideration, since this would imply a disproportionate and illegitimate use. In the case of those that act in a deferred manner, greater discretion is left to the agents, establishing only that the use they make must be proportionate and legitimate, when strictly necessary and selective. Therefore, the situations and moments in which such mechanisms can be used are not specified, and they can be deployed when not required and lead to a disproportionate use of the FRs. In view of the above, the purposes for which both types of mechanisms can be used must be strictly established, limited to those specified by the AIA for those that carry out identification in real time.

TWENTY-FIRST. The mere detection of the face by the system and the storage of data by the LEAs violates the protection of personal data.

The principle of data minimization is jeopardized by the use of FRs because huge amounts of data are needed, which must also be varied, for the proper training and construction of the watchlists used by the mechanism. The biggest problem derived from the above is that the mere detection of the face by the system, even if it is immediately eliminated, impacts the right to the protection of personal data because it is susceptible to being included in a database, as does the simple conservation of the same, due to the automated processing of facial information by the mechanisms. Therefore, whenever such systems are used, the right to the protection of personal data is violated because the simple capture of the face and the storage of the data cause this situation.

TWENTY-SECOND. The impact of FRs on identity occurs for two reasons: the redefinition of the face in terms of information in the digital sphere and its relation with privacy, given that interference in the latter impacts the former.

The face is an essential part of one's identity because it allows the person to identify oneself and others. The construction of identity is closely linked to privacy because the former is shaped by the interaction of the individual with the environment and with others. Video surveillance systems and, ultimately, the FRs inserted in them, have caused the boundaries between public and private space to blur. Given this scenario, if people limit their contacts and activities due to the affectation of their privacy, the right to the formation of personality is being violated. Furthermore, any breach of privacy constitutes an attack on identity. In addition, biometrics redefines the body in terms of information in the digital realm, producing a "disembodiment" effect that reaches the very essence of the human being. This process takes place when the processing and digitalization, in this case, of the face, leads to the simplification and reduction of the individual to a number, to an object that can be subsequently used by biometric systems to perform identification tasks. Thus, it impacts the very nature of people due to the dehumanization that it entails. Therefore, personal identity is altered by FRs due to the relationship between the former and privacy, since the impact on the latter reaches the identity itself and due to the redefinition of the face, since, by reducing it to a simple digit used by others, it causes the dehumanization and objectification of the individual.

TWENTY-THIRD. The impact on one's own image is produced by its relation to personal identity, privacy and dignity, although it is a right in need of specific protection.

Since FRs in the field of compliance with the Law can use the image of the face without the consent of the owner, the latter loses control of the right to his or her own image, which remains in the hands of third parties, who could use it even against the will of the former. The image itself and its protection are closely linked to personal identity, privacy and dignity. This is because the former aims to safeguard the ability to decide

which aspects of the image are to be kept hidden, in order to guarantee a private sphere for the proper development of the personality, free from interference from third parties. On the other hand, personal identity deserves special protection as an autonomous right, since the way it is understood has changed due to technological development. Thus, the face has acquired a new meaning or function, allowing communication in the digital environment. The parameters of the face are not only codified but also carefully prepared to be read and identified by the mechanisms along with the large amount of information they contain. For all the above reasons, one's own image, as a right linked to others but also autonomous, deserves specific protection.

TWENTY-FOURTH. The ability to monitor citizens, especially with deferred systems, impacts on freedom of movement.

FRs allow individuals to be identified by their facial parameters, but not only that, they go further and allow the location of a person to be known at a specific time, whether present or future, which can lead to the monitoring of their movements. The use of these not only allows the location to be known but, in a data aggregation process, it favours the knowledge of other aspects such as political or religious ties. This situation has a strong intimidating effect on individuals, who will decide not to carry out certain activities or movements for fear of being identified at any time and place, which is why they impact on freedom of movement, especially those who act in delayed mode due to the monitoring and surveillance capacity they imply.

TWENTY-FIFTH. FRs, regardless of the time taken to carry out identification, limit the right of expression in its aspects of assembly, association and strike and, therefore, affect the values of democratic society.

Peaceful meetings and demonstrations play an essential role in a democratic society because they are a means of exercising other rights and influencing public policy. FRs impact these because the registration of all participants in demonstrations and protests increases the capacity of the authorities to monitor these events and selectively track participants, either in real time or delayed, reducing or eliminating anonymity, which discourages citizens from exercising this right. Thus, these systems have a strong impact on the aforementioned rights and even affect the values of democracy.

TWENTY-SIXTH. The prohibition of discrimination is one of the rights most affected by the use of biometrics, specifically facial recognition, due to errors and biased results, as it is not a technique that provides greater objectivity to identification.

Since FRs process large amounts of data, using them carries a high risk of generating false results that contain biases and, as a result of this situation, discrimination. To ensure fairness, the use of biased or discriminatory applications and results must be reduced to a minimum.

The problem is that AIs often present inherent biases from their creators, which is why the results are not completely reliable and, from the interpretation made of them, prejudices and discrimination can arise. In relation to the FRs, as a mechanism that learns to recognize the faces of individuals through the set of images used for its training, it will better detect the parameters most represented in the dataset. There is also a margin of error when a match occurs, given that we are dealing with probabilistic mechanisms, whose results are not completely precise and concrete. For this reason, they cannot be considered accurate.

On the other hand, although they are seen more objective than human decisions, by acting using mathematical functions, they can produce biased and erroneous results, thus offering a false sense of objectivity, facilitating the perpetuation and amplification of existing discrimination through the mass identification they carry out. These mechanisms detect certain facial characteristics better than others, so they are more skilled at identifying certain profiles, being especially discriminatory in relation to race and gender. This is because they capture, for example, the profile of a white male better than a black one and a woman, as well. Based on this, due to errors and biased results, the prohibition of discrimination is one of the rights that is most affected by the use of FRs, not being a mechanism that provides greater objectivity in the identification process in the area of compliance with the Law.

TWENTY-SEVENTH. The rate of false positives in uncontrolled environments is very high and its results are much more damaging than false negatives because the incorrect identification of an individual leads to the start of a police investigation.

Erroneous results can be false positives and negatives. The latter imply the non-detection of a suspect by the system, while the former lead to the identification of a person as one of those contained in the watchlist and, therefore, the object of a police search for a suspected criminal or terrorist when, in reality, he or she is not. In addition to impacting the reputation of the individual, a situation of discrimination is created when the incorrect identification has occurred due to issues related to race or gender. The use of FRs in situations and environments which are uncontrolled drastically increases the rate of erroneous results and their consequences, even when the error rate of the mechanism in question is low, since it is capable of identifying an indefinite and very high number of people. Consequently, the effects of systems in this type of areas are very high and damaging, especially in relation to false positives, since they can lead to the initiation of a police investigation of innocent people based on certain categories of people, that is, those most frequently identified by the mechanism, even if incorrectly, perpetuating discrimination.

TWENTY-EIGHTH. Black boxes encourage discrimination and collide with the principle of transparency. The latter can be solved if the requirement of human intervention in decision-making is met.

In order to avoid discrimination, FRs must be mechanisms with a very high level of precision. The problem arises when, the greater the precision of the system, the greater the difficulties in understanding the way in which a certain decision has been made, making it also difficult to know and mitigate the vulnerabilities of the system and the biases. This situation also impacts the principle of transparency because the mechanism may be protected by trade secrets or it is difficult to understand the way the instrument works due to its technical complexity. For this reason, rather than the complete transparency of the system, the intervention of the person responsible for the mechanism must be guaranteed so that no one is subject to an exclusively automated decision, favouring the understanding of the results. Therefore, black boxes contribute to perpetuating and increasing discrimination and hinder the guarantee of the principle of transparency that must govern all automated data processing. However, to facilitate the understanding of the decision issued by the instrument, the involvement of the person responsible for its use in the decision-making process must be ensured, which facilitates the understanding of the decision even if the entire process followed for issuing the result is not known.

TWENTY-NINTH. The presumption of innocence is particularly affected in the initial phase of the police investigation by the use of FRs.

The presumption of innocence is one of the rights of citizens that is most compromised by the use of FRs and the danger of mass surveillance that they entail. This is because all citizens are considered potential suspects by the instrument and are susceptible to becoming the object of police surveillance without there being any suspicion on them or a warrant. In addition to the above, two serious problems that arise from algorithmic results are, on the one hand, the ability to act as decisive evidence in the judicial process; and, on the other, the reversal of the burden of proof. The latter occurs when the guilt of an individual is presumed when he is identified as one of those included in the watchlist and, presuming his guilt, he will be responsible for proving that the mechanism issued an erroneous result. Thus, there is a change from the presumption of innocence to a presumption of guilt. All the reasons mentioned lead us to conclude that the presumption of innocence is seriously threatened by the use of FRs in the field of law enforcement.

THIRTIETH. The exercise of rights is not absolute and may be limited by the interest in preventing and controlling crime according to the criteria of legal provision, proportionality and strict necessity in a democratic society. FRs are not a measure that meets all the requirements for this and, as there are other measures less restrictive of rights, they should not be used except in the case of the selective search for victims.

Rights may be limited when there is another interest at stake, as is the case with the prevention and control of crime. The first of the criteria by which their exercise may be limited is the existence of a specific legal basis in the internal regulatory system of

each country. If there is no such basis, the simple use FRs is *per se* a violation of rights without the need to observe other aspects. This principle does not only require the existence of a rule that provides for the use of such mechanisms, since it must meet certain requirements related to quality, accessibility and predictability for citizens. Thus, it must include an adequate indication of the conditions and circumstances that enable the authorities to adopt this instrument restricting rights. Among them, the norm must specify the types of crimes to which they are applicable and the appropriate threshold of seriousness of the same to exclude common crime from its scope of action. In addition, the express provision of guarantees and measures to ensure a rational use of them is added. The AIA establishes these issues, at least in relation to real-time RBIS, having to wait for the States to introduce them in their internal regulations to know the way in which they will be deployed, since that is not the legal basis. For that reason, *ad hoc* regulations are necessary that act as such, both for these and those that operate in deferred time.

That a measure is legally provided for is not a sufficient criterion for its implementation. Thus, the proportionality test appears as the guiding principle in the specification of the limitation of rights. In the case of crime prevention and control through FRs, high standards of protection must be established by analysing compliance with the three dimensions that make up this requirement. Thereby, these systems can only be used when the goal cannot be achieved with other less intrusive measures. The costs in terms of citizens' rights and freedoms are very high, while the maintenance of security through the prevention of crime, including serious crime, is already adequately guaranteed by conventional video surveillance systems. Therefore, since there is a less restrictive measure than those, FRs should not be used in this field, as it is not proportional.

Despite what has been immediately pointed out, in order to implement the mechanisms, the principle of strict necessity in a democratic society must also be observed. In this case, they must have the safeguards and guarantees to prevent abuse, which in turn depends on the circumstances of the case. The inclusion of the adverb "strictly" requires observing more severe conditions than simple necessity, which restricts the margin of appreciation, and the circumstances and conditions of its use must be defined according to objective criteria. In our field, strict necessity is linked to the exceptional situations established in the AIA to lift the ban on the use of real-time FRs. As for the selective search for missing persons and victims of certain crimes, it is an appropriate measure for the purpose pursued given the difficulty of finding these people, to which are added issues relating to immediacy and speed to avoid greater harm to them. The last two assumptions correspond to the existence of a specific, important and imminent threat to the life or physical safety of people or a real and current or real and foreseeable threat of a terrorist attack; and the location of suspects of having committed a serious crime. In both cases, it is understood that recourse to the FRs is legitimate due to the importance of maintaining national security and, given that terrorism and serious crime seriously harm it, a greater interference in rights is justified.

In spite of this and the restrictions established in the AIA, the State is left with a wide margin of discretion when deciding whether to implement it, which may lead to arbitrary actions, especially with delayed systems, since the requirements and guarantees for their use are less strict. Therefore, since the impact on citizens' rights and freedoms is very high compared to the expected benefits, FRs should not be deployed in the area of crime control and prevention, since there are other measures that are less restrictive of rights and equally effective. However, it is necessary and justified in a democratic society to use them as a mechanism to identify victims of certain crimes and missing persons, since, in this specific case, the benefits are higher compared to the risks, since they do not entail the initiation of a criminal process.

THIRTY-FIRST. The fact that the AIA allows the use of FRs in certain situations may lead to its extension to situations other than those initially planned.

With the provision made by the AIA for the use of FRs in some situations for which certain guarantees must be observed, it may lead to the expansion of its use to other circumstances that do not require it. This is especially dangerous when the requirement of prior authorization may not be met in cases of urgency and necessity. This offers a wide margin of appreciation and discretion to the agents in charge of its implementation, who could resort to these systems in situations that do not require it, alleging such circumstances. Likewise, the range of individuals susceptible to being the object of the measure may be extended and go beyond those initially planned and even reach innocent citizens. Other controversial issues in relation to the function creep are the change or extension of the databases, the increase in the range of users and the possible extension to other areas and places. Therefore, the fact that the AIA allows the use of FRs, both in delayed and in real time, even though it limits the former to certain situations and under certain circumstances and conditions, may lead to an extension of the same to other situations different than those for which it was intended, which do not require it and, therefore, a use of this technique is being made that is not legally foreseen. In those that act in deferred mode this is even worse, given that the situations in which they can be used are not specifically mentioned, and may even reach common crime.

THIRTY-SECOND. The expansion of FRs can lead to a situation of mass surveillance, causing inequalities and power imbalances.

The collection and use of biometrics carries a risk of hyper-surveillance of citizens. Those who use FRs have a great power over others, and imbalances exist. As it is a technology that invades rights and freedoms, it can cause a feeling of constant surveillance that indirectly discourages their exercise, all under the argument of providing greater security, when there are no studies that demonstrate the increase in the latter a cause of the use of those. Therefore, if the use of FRs spreads, it can lead to mass surveillance of the population, through their location, monitoring and profiling, which leads to inequality between those who use them and the individuals being monitored, as well as power imbalances between the two.

THIRTY-THIRD. The threat to security posed by current terrorism and crime has led to a decrease in the subjective feeling of security and, for this reason, society demands the adoption of preventive measures, legitimizing the use of FRs for this purpose.

In the risk society in which we live, there is concern about the incidents that may be committed in the future, especially terrorist acts and serious crime that threaten security. To prevent such incidents, new technologies are used, including FRs. Citizens may legitimize the use of these technologies because they consider that this prevents the commission of crimes, even if it involves intrusive surveillance. The new instruments for crime prevention have a symbolic rather than an effective role, since what they aim to do is increase the subjective perception of security among citizens. Likewise, the population demands and legitimizes the use of preventive measures such as FRs because they feel safer and more protected against risks that endanger security, at the expense of their own rights and freedoms.

THIRTY-FOURTH. The mission of the police is to maintain security and prevent crime. It has the ability to decide the most appropriate measures for this, which allows it a wide margin of discretion that reduces predictability and can lead to an arbitrary exercise of functions that must be avoided.

The State delegates to the police the function of repression and prevention of crime and, consequently, the maintenance of security. Agents have a wide margin of appreciation and can choose in a given situation the most appropriate measure or measures, and may even be the FRs. This causes the reduction of the element of predictability, which is fundamental to assess whether an instrument is adequate and does not exceed the limits of rights, especially when the actions are secret and the individuals involved do not know the deployment of the measure so as not to hinder police work. All of this is problematic because it can lead to an arbitrary use of police functions that leads to mass surveillance, so measures must be adopted to avoid it.

THIRTY-FIFTH. Security is a requirement for the exercise of other rights. The police have the obligation to maintain it by using appropriate mechanisms to achieve legitimate aims. Effective controls are necessary to ensure the balance between freedom and security.

The police have the obligation to act when a real and immediate risk of violation of citizens' rights by the commission of a crime is observed. They may use electronic mechanisms to do so, including FRs. However, they cannot make abusive and illegitimate use of them and the population must be protected. For this reason, it is necessary to carry out effective controls of the measures adopted and to guarantee a balance between both values.

THIRTY-SIXTH. Security is the argument used to justify the use of FRs, but the real impact they have on security is unknown, and so it is not a sufficient reason to implement these mechanisms.

The defendants of the implementation and development of FRs in terms of compliance with the Law allude to the argument that these mechanisms have very high benefits in terms of security. However, this is practically impossible to affirm due to the absence of empirical studies that provide conclusive results. Therefore, in the absence of information, the real impact that FRs have on security is unknown, and the latter is not a sufficient and justified reason to implement such systems.

THIRTY-SEVENTH. FRs facilitate social control.

The creation and processing of data on a massive scale has led to the emergence of a new type of mass surveillance that uses data. FRs interfere with the lives of citizens, in the sense of restricting their movements. This situation is caused by the discreet action of these mechanisms inserted in CCTV, which means that surveillance can take place at any time without the knowledge of individuals. The fact of knowing that one can be the object of surveillance but not knowing when and by whom, leads to the emergence of a feeling of constant surveillance. The above leads to the conclusion that FRs facilitate social control.

THIRTY-EIGHTH. FRs can become banal objects in the maintenance of security and lead to a situation of digital panopticon.

The increasingly widespread use of technologies in everyday life means that they are seen as common and, therefore, banal and harmless. Currently, FRs are not so common, which is why their risks continue to be considered. However, due to their use in electronic devices as an instrument to verify identity and to be able to access them, as well as in the field of security, society is becoming less and less aware of the dangers they entail. Thus, they are not subject to public debate or scrutiny. On the other hand, the expansion of these and CCTV in public spaces results in the subjection of society to a type of invisible, impersonal, general surveillance, without a specific objective. This situation causes the monitoring of citizens, tacitly and implicitly, in a kind of digital panopticon, in which the movements of citizens can be observed and controlled. Therefore, FRs can become banal instruments and provoke a situation of digital panopticon that favours the exercise of mass surveillance in society.

THIRTY-NINTH. With the regulation of FRs in the public space for the purposes of compliance with the Law, the AIA is allowing their widespread use in the European Union. There is a risk of an intolerable violation of rights and freedoms and a possible drift towards a state of mass surveillance.

As a final conclusion, general to the all investigation, it should be noted that the regulation of FRs in the AIA for the purposes of compliance with the Law in the public space is opening the door to their widespread use in the European Union, rather than

restricting it. Regarding the systems that act in a delayed manner, it does not establish specific and limited requirements and conditions, and they can even be used in situations of common crime, being likely to violate the rights and freedoms of citizens in an intense way. As regards those that operate in real time, even though the times and requirements in which they may be used are more specifically determined, a wide margin of discretion is left to the agents to decide when to use them, which may lead to a disproportionate and irrational use of this mechanism, especially when the arguments of urgency and necessity are used to avoid requesting prior authorisation. For all the above reasons, it can be concluded that the regulation of the FRs by the AIA, rather than prohibiting them, is allowing a broad and extended use of them in the Union, thereby putting the exercise of rights and freedoms at intolerable risk, and may even lead to a state of mass surveillance, under the pretext of increasing security.

BIBLIOGRAPHICAL APPENDIX

BIBLIOGRAPHY

AARVIK, P., *Artificial Intelligence-a promising anti-corruption tool in development settings?*, U4. Anti-corruption Resource Centre, Chr. Michelsen Institute, 2019.

ABAZA, A. et al. "A Survey on Ear Biometrics", *ACM Computing Surveys*, vol. 45, nº. 22, 2013, pp. 1-35.

ACOSTA GUZMÁN, H.M. "Lineamientos estratégicos para combatir los Grupos Armados Organizados en el escenario pos-acuerdo", in Payá Santos, C.A. (Dir.), *La gestión del riesgo. La inseguridad jurídica y las amenazas a la seguridad*, Aranzadi, Navarra, 2020, pp. 103-124.

ADINOLFI, A. "L'Intelligenza Artificiale tra i rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro nomativo dell'Unione", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 127-163.

AHMED, S.I. et al. "Privacy, security and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh", *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 906-918.

AKHTAR, M. "Police use of facial recognition technology and the right to privacy and data protection in Europe", *Nordic Journal of Law and Social Research*, nº. 9, 2019, pp. 325-344.

ALBA CATOIRA, A. "La garantía de los derechos como respuesta frente a los retos tecnológicos", in Balaguer Callejón, F. & Cotino Hueso, L. (Dirs.), *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, pp. 57-84.

ALBRIZIO, A. "Biometry and Anthropometry: from Galton to Constitutional Medicine", *Journal of Anthropological Sciences*, vol. 85, 2007, pp. 101-123.

ALDERSON, J. *Human Rights and the Police*, Council of Europe, Strasbourg, 1984.

ALGERI, L., "Giustizia predittiva: itelligenza artificiale e processo penale", en Adinolfi, A. & Simoncini, A. (Dirs.), *Protezione dei dati personali e nuove tecnlogie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizione Scientifiche Italiane, Napoli, 2022, págs. 653-677.

ALGHAMDI, S.M. et al. "Enhancing security in multimodal biometric fusion: Analyzing adversarial attacks", *IEEE Access*, vol. 12, 2024, pp. 1-13.

ALLEWELDT, R. & FICKENSCHER, G. "Introduction: The police, a key actor in human rights protection", *The police and international human rights law*, Springer, 2018, pp. 1-5.

ALONSO SALGADO, C. "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *Ius et Scientia*, vol. 7, nº. 1, 2021, pp. 25-36.

AMONI REVERÓN, G.A. "Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal", in Cotino Hueso, L. (Dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, pp. 193-236.

ANDREJEVIC, M. "Ubiquitous surveillance", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 91-98.

ANIK, M.A.H. et al. "Investigation of pedestrian jaywalking behaviour at mid-block locations using artificial neural networks", *Safety Science*, vol. 144, 2021, pp. 1-11.

ARCHARD, D. "The value of privacy", in Claes, E. et al. *Privacy and the Criminal Law*, Intersentia, Antwerpen, 2006, pp. 13-31.

ARENAS RAMIRO, M. & DÍAZ LIMA, D. "Privacidad y derechos digitales", in Balaguer Callejón F. & Cotino Hueso, L. (Coords.), *Derecho público de la Inteligencia Artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios del Estado Autonómico, Zaragoza, 2023, pp. 287-317.

ARTICLE 29 DATA PROTECTION WORKING PARTY*: Opinion 3/2012 on developments of biometric technologies*, 00720/12/EN WP103, 27 de abril 2012.

- *Opinion 03/2013 on Purpose Limitation*, WP 2013, 00569/13/EN, Bruxelles, 2 April 2013.
- *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, 29 de noviembre de 2017.

ASHRAF, C. "Exploring the impacts of artificial intelligence on freedom of religion or belief online", *The International Journal of Human Rights*, vol. 26, nº. 5, 2022, pp. 757-791.

ASIT, K.D. & PRIYANKA, D. "Graph based ensemble classification for crime report prediction", *Applied Soft Computing*, nº. 125, 2021, pp. 1-14.

ATIENZA, M. *Sobre la dignidad humana*, Editorial Trotta, Madrid, 2022.

AYERBE, A. "La ciberseguridad y su relación con la inteligencia artificial", *Real Instituto Elcano*, nº. 128, 2020, pp. 1-8.

BAJC, V. "Sociological reflections on security through surveillance", *Sociological Forum*, vol. 28, nº. 3, 2013, pp. 615-623.

BALAGUER CALLEJÓN, F. & COTINO HUESO, L. (Coords.), *Derecho público de la Inteligencia Artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios del Estado Autonómico, Zaragoza, 2023.

BAO, J. et al. "Towards Open-Set Identity Preserving Face Synthesis", *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 6713-6722.

BARKANE, I. "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance", *Information Polity*, nº. 27, 2022, pp. 147-162.

BARKER, R.B. "A definition of privacy", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, pp. 275-296.

BASILE, F. "Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione", in Balbi, G. et al. (Dirs.), *Diritto penale e Intelligenza artificiale "nuovi scenari"*, G. Giappichelli Editore, Torino, 2022, pp. 1-17.

BASSINI, M. & POLLICINO, O. "Intelligenza artificiale e protezione dei dati personali", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 269-279.

BEHRENSEN, M. "Identity as convention: Biometric Passports and the promise of security", *Journal of Information, Communication and Ethics in Society*, vol. 12, nº. 1, 2014, pp. 44-59.

BEIGNER, B. "La protection de la vie privée", in Cabrillac, R. et al. (Dirs.), *Libertés et droits fondamentaux*, Dalloz, Paris, 2007, pp. 179-204.

BERNAL BALLESTEROS, M.J. "La función policial desde la perspectiva de los derechos humanos y la ética pública", *IUS. Revista del Instituto de Ciencias jurídicas de Puebla, México*, vol. 13, nº. 44, 2019, pp. 251-279.

BERNAL DEL CASTILLO, J. "Prevención y seguridad ciudadana. La recepción en España de las teorías criminológicas de la prevención situacional", *Revista de Derecho Penal y Criminología*, nº. 9, 2013, pp. 267-304.

BLEDSOE, W.W. "Man-Machine facial recognition: Report on a large-scale experiment", *Technical Report PRI: 22*, Panoramic Research Inc. Palo Alto, CA, 1966.

BLOUNT, K., "Using artificial intelligence to prevent crime: implications for due process and criminal justice", *AI & Society*, 2022, pp. 1-10.

BOGARD, W. "Simulation and post-panopticism", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 30-37.

BREY, P. "Ethical aspects of facial recognition systems in public places", *Journal of Information, Communication and Ethics in Society*, vol. 2, nº. 2, 2004, pp. 97-109.

BROADHURST, R. et al. *Artificial Intelligence and Crime. A Research Report for the Korean Institute of Criminology and the Australian National University Cybercrime Observatory*, 2018.

BUDAK, J. et al. "Citizens' privacy concerns. Does national culture matter?", in Friedewald, M. et al (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, pp. 36-51.

BUCHER, T. "Facing AI: conceptualizing 'fAIce communication' as the modus operandi of facial recognition systems", *Media, Culture & Society. Special Issue: Reclaiming the human in machine cultures*, vol. 44, nº. 4, 2022, pp. 638-654.

BUOLAMWINI, J. & GEBRU, T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research*, vol. 81, 2018, pp. 1-15.

BURTON, A.M. et al. "Face recognition in por-quality video: Evidence form security surveillance", *Psychological Science*, vol. 10, nº. 3, 1999, pp. 243-248.

BUSTOS RAMÍREZ, J. "Las funciones de la policía y la libertad y seguridad de los ciudadanos", *Nuevo Foro Penal*, nº. 32, 1986, pp. 165-177.

BUTT, U.M. et al. "Spatio-Temporal Crime Predictions by Leveraging Artificial Intelligence for Citizens Security in Smart Cities", *IEEE Access*, vol. 9, 2021, pp. 47516-47529.

BYK, C. "Biométrie et Constitution: est-il déjà trop tard pour les libertés publiques?", *La Semaine Juridique-Édition Generale*, nº. 25, 2008, pp. 19-22.

CANO PAÑOS, M.A. "La amenaza proveniente de los combatientes yihadistas retornados a España, ¿Motivo de preocupación?", *Revista de Estudios de Seguridad Internacional*¸ vol. 8, nº. 2, 2022, pp. 189-203.

CARVAJAL IBARRA, L.P. & ANDRADE ULLOA, D.L. "Impacto de la tecnología de reconocimiento facial en la prevención del crimen", *Anatomía Digital*, vol. 7, nº. 2.2, 2024, pp. 209-221.

CARVAJAL MARTÍNEZ, J.E. "El paradigma de la seguridad y las tensiones con los derechos humanos", *Utopía y Praxis Latinoamericana*, vol. 23, nº. 1, 2018, pp. 97-108.

CASADEVALL, J. *El Convenio Europeo de Derechos Humanos, el Tribunal de Estrasburgo y su jurisprudencia*, Tirant lo Blanch, Valencia, 2012.

CAS, J. et al. "Introduction. Surveillance, privacy and security", in Friedewald, M. et al (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, pp. 1-12.

CASTALDO, M.E. & NADDEO, M. "Sicurezza e controllo prevenzionale. Le misure di prevenzione tra passato e futuro", in Forgione, A. et al. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milán, 2020, pp. 104-128.

CASTETS-RENARD, C. & TURCI, A. "'Caméras augmentées': un danger pour les libertés lors des Jeux Olimpiques et Paralimpiques, et au-delà?", *Recueil Dalloz*, nº. 22, 2023, pp. 1138-1141.

CEPEDA HERNÁNDEZ, A.J. "Garantías de la seguridad ciudadana en el marco del apoyo de las Fuerzas Armadas a la Policía Nacional de República Dominicana en un marco de Seguridad y Defensa", in Payá Santos, C.A. (Dir.), *La gestión del riesgo. La inseguridad jurídica y las amenazas a la seguridad*, Aranzadi, Navarra, 2020, pp. 125-138.

CERF, A. "Ordre public, Droit pénal, et droits fondamentaux", in Redor, M.J (Dir.), *L'ordre public: Ordre publico u ordres publics? Ordre public et droits fondamentaux*, Bruylant, Bruxelles, 2001, pp. 63-83.

CEYHAN, A. "Surveillance as biopower", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 38-45.

CHANGO, X. et al. "Technology in forensic sciences: Innovation and precision", *Technologies*, vol. 12, nº. 120, 2024, pp. 1-25.

CHAZAL, G. *Du panoptique de Bentham à la surveillance numérique*, Éditions Universitaires de Dijon, Collection Essais, Dijon, 2024.

CHEN, S. et al. "Face Recognition from Still Images to Video Sequences: A Local-Feature-Based Framework", *EURASIO Journal on Image and Video Processing*, vol. 2011, 2011, pp. 1-14.

CHESTERMAN, S. "Artificial Intelligence and the limits of legal personality", *International and Comparative Law Quarterly*, vol. 69, 2020, pp. 819-844.

CHOWDHRY, A. et al. "The pitfalls of surveillance technology: Policy analysis and solutions", *Institute for Youth in Policy. Policy Department I Brief*, 2023, pp. 1-5.

CIAMPI, M. "Is 'security state' come paradigma della statualità contemporanea", en Forgione, A., Massucci, R., y Ferrigni, N. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milano, 2020, pp. 94-103.

CLARK, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues", *Information Technology & People*, nº. 7-4, 1994, pp. 6-37.

COFFIN, J.S. & INGRAM, D. *Facial recognition system for security Access and identification*, Patente de Estados Unidos, nº 5.991.429, Washington DC: Oficina de Patentes y Marcas de los Estados Unidos, 1999.

COGHLAN, N. "*Gaughran* [2015] UKSC 29 on police biometric data retention: Strasbourg unheard, Strasbourg unheeded", *European Human Rights Law Review*, nº. 21, 2016, pp. 61-72.

COLACURI, M. "Riconoscimento faciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini", in Balbi, G., et al, (Dirs.), *Diritto penale e intelligenza artificiale "nuovi scenari",* G. Giappichelli Editore, Torino, 2022, pp. 119-144.

COMEST, *Preliminary Study on the Ethics of Artificial Intelligence*, Paris, 2019.

COPELAND, J. *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life: Plus The Secrets of Enigma*, Oxford University Press, New York, 2004.

CORALLO, M. "Electronic Monitoring as an electronic panopticon: A Foucauldian perspective", *Manchester Review of Law, Crime and Ethics*, vol. 10, 2021, pp. 110-120.

CORVALÁN, J.G. "La primera inteligencia artificial predictiva al servicio de la justicia: *Prometea*", *La Ley*, nº. 186, 2017, pp. 1-12.

COTINO HUESO, L.: "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata*, nº. 24, 2017, pp. 131-150.

- "Nuevo paradigma de las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", in Cotino Hueso, L. (Dir.), *Derecho y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, pp. 67-105.
- "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, nº. 63, 2023, pp. 1-22.
- "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", *El Cronista del Estado Social y Democrático de Derecho*, nº. 100, 2023, pp. 68-79.
- "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", in Balaguer Callejón, F. & Cotino Hueso, L. (Coords.), *Derecho Público de la Inteligencia Artificial*, Fundación Manuel Jiménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, pp. 347-402.

COUCHMAN, H. "Mass Surveillance on Our Streets: Facial Recognition and the Threat to Our Rights", *European Human Rights Law Review*, nº. 6, 2019, pp. 585-589.

CRAWSHAW, R. "Introduction to the seminar on human rights and the police: Human rights, the rule of law and policing", in *Human Rights and the Police. Seminar proceedings, Strasbourg 6-8 December, 1995*, Council of Europe Publishing, 1997, pp. 11-20.

CROSS, C. "Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging", *Crime Prevention and Community Safety*, vol. 23, 2022, pp. 30-41.

CUERDA ARNAU, M.L. "La reforma de Ley de Enjuiciamiento Criminal en materia de tecnovigilancia. Visión de conjunto", in Alonso Rimo, A. et al. (Dirs.). *Terrorismo, sistema penal y derechos fundamentales*, Tirant lo Blanch, Valencia, 2018, pp. 509-542.

DACOBA CERVIÑO, F.J. "Prólogo" a FERNÁNDEZ RODRÍGUEZ, J.J. *Seguridad (es) en un futuro incierto (un estudio jurídico constitucional)*, Aranzadi, Navarra, 2020.

D'ALOIA, A. "Ripensare il Diritto nel tempo dell'Intelligenza Artificiale", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 79-110.

DAUVERGNE, P. *Identified, tracked, and profiled: The politics of resisting facial recognition technology*, Edward Elgar Publishing, 2022.

DAWES, J. "Speculative human rights: Artificial Intelligence and the future of humans", *Human Rights Quarterly*, nº. 42, 2020, pp. 573-593.

DE BEER, D. et al. "Nouveaux éclairages de la notion de 'donnée personnelle' et application audacieuse du critère de proportionalité", *Revue trimestrielle des droits de l'homme*, nº. 21, 2010, pp. 141-161.

De HERT, P. "Biometrics: legal issues and implications", *Background Paper for the Institute of Prospective Technological Studies, DG JRC–Sevilla, European Commission*, 2005.

DE HOYOS SANCHO, M. "El uso jurisdiccional de los sistemas de Inteligencia Artificial y la necesidad de su armonización en el contexto de la Unión Europea", *Revista General de Derecho Procesal*, nº. 55, 2021, pp. 1-29.

DE LA CORTE IBÁÑEZ, L. & BLANCO, J.M. "Potenciadores del riesgo. Una visión ampliada para un mundo global", in De la Corte Ibáñez, L. & Blanco Navarro, J.M. (Dirs.), *Seguridad Nacional, Amenazas y Respuestas*, Lid Editorial, Madrid, 2014, pp. 55-78.

DE LA MATA BARRANCO, N.J. & BARIÑAS UBIÑA, D. "La protección penal de la vida privada en nuestro tiempo social: ¿Necesidad de redefinir el objeto de tutela?", *Revista de Derecho Penal y Criminología*, nº. 11, 2014, pp. 13-92.

DELEUZE, G. "Postscript on the societies of control", *Surveillance, crime and social control*, Routledge, 2017, pp. 35-39.

DERAVI, F. "Intelligent Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 177-191.

DÍAZ RODRÍGUEZ, V. "Sistemas biométricos en materia criminal: un estudio comparado", *Revista del Instituto de Ciencias Jurídicas de Puebla*, nº. 31, 2013, pp. 28-47.

DI RAIMONDO, M. *Ordine pubblico e sicurezza pubblica. Profili ricostruttive e applicative*, G. Giappichelli Editore, Torino, 2010.

DOCKSEY, C. "Articles 7 and 8 of the EU Charter: Two distinct fundamental rights", in Grosjean, A. (Dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, Bruxelles, 2015, pp. 71-97.

DOMINGO JARAMILLO, C.: "Aplicación del sistema de reconocimiento facial para prevenir la violencia asociada al deporte en los encuentros calificados de alto riesgo", in Calaza López, S. & Llorente Sánchez-Arjona, M. (Dirs.), *Inteligencia artificial legal y administración de justicia*, Aranzadi, Navarra, 2022, pp. 125-150.

– "Aproximación a la aplicación de sistemas de inteligencia artificial para prevenir la corrupción en la administración pública", *Cuadernos de Política Criminal*, nº. 140, 2023, pp. 105-134.

DONADL, A. "The implementation of European Court of Human Rights Judgments against the UK: Unravelling the paradox", in Ziegler et al. (Dirs.), *The UK and European Human Rights. A strained relationship?*, Hart Publishing, 2015, pp. 135-162.

DONATI, F.: "Introduzione. Il percorso della ricerca", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 27-39.

– "Diritti fonamentali e algoritmi nella proposta di Regolamento sull'Intelligenza Artificial", in Pajno, A. et al. (Dirs.), *Intelligenza Artificiale e diritto: una rivoluzione?*, il Mulino, Bologna, 2022, pp. 111-126.

DROSOU, A. & TZOVARA, D. "Activity and Event Related Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 129-149.

DUBUISSON, F. "La Cour Européenne des Droits de l'Homme face à la surveillance de masse (obs. sous Cour Eur. Dr. H., Gde Ch., arrêt Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021), *Revue Trimestrielle des Droits de l'Homme*, nº. 129, 2022, pp. 123-141.

DUFFY, P. "Case-law under the European Convention of Human Rights relevant to the police", in *Human Rights and the Police. Seminar proceedings, Strasbourg 6-8 December, 1995*, Council of Europe Publishing, 1997, pp. 21-38.

DUSHI, D. "The use of facial recognition technology in EU law enforcement: Fundamental rights implications", *Global Campus of Human Rights. South East Europe*, Policy Briefs, 2020.

EDPB: *Guidelines 3/2019 on processing of personal data through video devices*, version 2.0, adopted on 29 January 2020.

- *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 1.0*, adopted on 12 May 2022.
- *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0*, adopted on 26 April 2023

EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 June 2021.

EDPS: *Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II)* (Com(2005) 236 final y COM(2005) 237 final), OJ C 91,19.4.2006.

- *Opinion of 18 July 2013, on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP).*
- *Opinion 4/2015 Toward a new digital ethic. Data, dignity and technology*, 2015.
- *Opinion of 3/2016 of 13 April 2016, on the Exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS).*
- *Opinion 07/2016 on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin Regulations).*
- *Opinion of 7/2018 of 10 August 2018, on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents.*

EIREINER, A.V. "Imminent dystopia? Media coverage of algorithmic surveillance at Berlin-Südkreuz", *Internet Policy Review. Journal of Internet Regulation*, vol. 9, nº. 1, 2020, pp. 1-19.

ELMER, G. "Panoptic-discipline-control", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 21-29.

EMANUELE, M. & FERRANTINO, T. "Rischio e complessità", in Forgione, A. et al. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milán, 2020, pp. 182-188.

ESCAJEDO SAN-EPIFANIO, L. *Tecnologías biométricas, identidad y derechos fundamentales*, Aranzadi, Navarra, 2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020.

FAIRHURST, M. et al. "Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data", *IET Biometrics*, vol. 6, nº. 6, 2017, pp. 369-378.

FELSON, M. & CLARKE, R.V. "Opportunity Makes the Thief. Practical theory for crime prevention", *Police Research Series, paper, 98*, 1998, pp. 1-36.

FERNÁNDEZ RODRÍGUEZ, J.J.: "El encuentro entre seguridad y derechos humanos: Actualidad y problemas", *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 14, nº. 1, 2019, pp. 87-101.

- *Seguridad (es) en un futuro incierto (un estudio jurídico constitucional)*, Aranzadi, Navarra, 2020.
- "¿Cómo responder a los desafíos de seguridad? Una aproximación desde la dogmática de los derechos fundamentales", en Godoy, O., (Coord.), *Libertad y Seguridad en un contexto global. Retos y desafíos para los sistemas de garantía de los derechos fundamentales*, Dykinson, Madrid, 2020, pp. 27-51.

FERRIGNI, N. "La sicurezza come metodo, il metodo nella sicurezza", en Forgione, A. et al. (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, FrancoAngeli, Milán, 2020, pp. 39-54.

FINKLEA, K. et al. "Federal law enforcement use of facial recognition technology", *Congressional Reseach Service*, 2020.

FINOCCHIARO, G. *Intelligenza artificiale. Quali regole?*, Il Mulino, Bologna, 2023.

FOUCAULT, M. *Discipline and punish*, A. Sheridan, Tr. Gallimard, Paris, 1975, pp. 1-26.

FRA: *Handbook on European non-discrimination law*, 2018.

- *Handbook on European data protection law, 2018 Edition*, Publication Office of the European Union, Luxembourg, 2019.
- *Data quality and artificial intelligence-mitigating bias and error to protect fundamental rights*, 2019.
- *Facial recognition technology: Fundamental rights considerations in the context of law enforcement*, 2020.

FRETTY, D.A. "Face-recognition surveillance: A moment of truth for fourth amendment rights in public places", *Virginia Journal of Law & Technology*, vol. 16, nº. 2, 2011, pp. 431-463.

FULCHIRON, H. et al. "Vie privée et familiale", *Journal Europeen des Droits de l'Homme*, nº. 1, 2021, pp. 242-270.

GABA, J.P.M. & ESTREMADURA, J.J.M. "Data protection of biometric data and genetic data", *Ateneo Law Journal*, vol. 64, 2019, pp. 949-982.

GABOR, T. et al. "Robust thermal face recognition for law enforcement using optimized deep features with new rough sets-based optimizer", *Journal of Information Security and Applications*, vol. 85, 2024, pp. 1-17.

GALETTA, A. "The changing nature of the presumption of innocence in today's surveillance societies: Rewrite human rights or regulate the use of surveillance

technologies?", *European Journal of Law and Technology*, vol. 4, nº. 2, 2013 (unpaginated).

GANDY, O. *The panoptic sort: A political economy of personal information*, Oxford University Press, 2021.

GARCÍA TOMA, V. "La dignidad humana y los derechos fundamentales", *Derecho & Sociedad*, nº. 51, 2018, pp. 13-31.

GATES, K.A. *Our biometric future: Facial recognition technology and the culture of surveillance*, vol. *2*, New York University Press, 2011.

GEARTY, C. "Escaping Hobbes: Liberty and security for our democratic (not anti-terrorist) age", in Reed, E.D. & Dumper, M. (Eds.), *Civil liberties, national security and prospects for consensus*, Cambridge University Press, Cambridge, 2014, pp. 35-61.

GERARDS, J. "The fundamental rights challenges of algorithms", *Netherlands Quarterly of Human Rights*, vol. 37, nº. 3, 2019, pp. 205-209.

GHILARDI, G. & KELLER, F. "Epistemological Foundation of Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 23-47.

GIL MEMBRADO, C. *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*. Wolters Reuters, Madrid, 2019.

GIROTTO, S. "Il trattamento dei dati biometrici", in Rodotà, S. & Zatti, P. (Dirs.), *Trattato di Biodiritto. Il governo del corpo, vol. I*, Giuffrè Editore, Milano, 2011, pp. 1237-1249.

GOBIERNO DE ESPAÑA, *Estrategia de Seguridad Nacional 2021*, Catálogo de publicaciones de la Administración General del Estado, 2021, Madrid.

GODOY, O. *Libertad y Seguridad en un contexto global. Retos y desafíos para los sistemas de garantía de los Derechos fundamentales*, Dykinson, Madrid, 2020.

GOH, M.K. et al. "Touch-less palm print biometrics: Novel design and implementation", *Image and Vision Computing*, vol. 26, nº. 12, 2008, pp. 1551-1560.

GONG, S. et al. "Security and Surveillance", in Moeslund, T.B. et al. (Eds.), *Visual analysis of humans. Looking at people*, Springer, 2011, pp. 455-472.

GOOLD, B. et al. "The banality of security. The curious case of surveillance cameras", *British Journal of Criminology*, vol. 53, nº. 6, 2013, pp. 977-996.

GORDON, B.J. "Automated facial recognition in law enforcement: The Queen (on application of Edward Bridges) v The chief constable of South Wales Police", *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, vol. 24, nº. 1, 2021, pp. 1-29.

GORDON, D.R. "The electronic panopticon: A case study of the development of the National Criminal Records System", *Politics and Society*, vol. 15, nº. 4, 1987, pp. 483-511.

GPDP, *Sistema automatico di ricerca dell'identità di un volto* [9040256], de 26 de julio de 2018.

GRM, K. et al. "Strengths and weaknesses of Deep learning models for face recognition against image degradations", *IET Biometrics. Special Issue: Face Recognition and Spoofing Attacks*, vol. 7, nº. 1, 2017, pp. 81-89.

GUNTURK, B.K. et al. "Eigenface-Domain Super-Resolution for Face Recognition", *IEEE transactions on image processing*, vol. 12, no 5, 2003, p. 597-606.

GUO, T. "Alan Turing. Artificial intelligence as human self-knowledge", *Antropology Today*, vol. 31, nº. 6, 2015, pp. 3-7.

GUO, Z. & KENNEDY, L. "Policing based on automatic facial recognition", *Artificial Intelligence and Law*, vol. 31, 2023, pp. 397-443.

GUTIERREZ SULLCA, E.M. "Artificial intelligence techniques for detecting deepfakes and their impact on the veracity of online content", *International Journal of Systems Engineering*, vol. 4, nº. 2, 2023, pp. 6-9.

HAGGERTY, K.D. "Surveillance, crime and the police", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 235-243.

HALE, B. "Identity crisis: face recognition technology and freedom of the will", *Ethics Place and Environment*, vol. 8, nº. 2, 2005, pp. 141-158.

HAMZAH, M.A. "Advancing personal identity verification by integrating facial recognition through deep learning algorithms", *International Journal of information Technology*, 2024, pp. 1-6.

HAYWARD, K.J. & MAAS, M.M. "Artificial intelligence and crime: A primer for criminologists", *Crime Media Culture*, vol. 17, nº. 1, 2021, pp. 209-233.

HERRERA, F. et al. "Una visión actual de la Inteligencia Artificial: recorrido histórico, datos y aprendizaje, y responsabilidad en el diseño y uso", in Peralta et al. (Coords.), *El derecho y la Inteligencia Artificial,* Editorial Universidad de Granada, Granada, 2022, pp. 51-79.

HERVERG, J. & VAN GYSEGHEM, J.M. "La protection des données à caractère personnel en droit européen- Chronique de jurisprudence (2020)", *Journal Europeen des Droits de l'Homme,* nº. 1, 2021, pp. 52-128.

HEVAL ÇINAR, O. "The current case law of the European Court of Human Rights on privacy: challenges in the digital age", *The International Journal of Human Rights*, vol. 25, nº. 1, 2021, pp. 26-51.

HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethichs Guidelines for Trustworthy AI*, 2019.

HILDEBRANDT, M. "Privacy and Identity", in Claes, E. et al. *Privacy and the Criminal Law*, Intersentia, Antwerpen, 2006, pp. 43-57.

HIRANANDANI, V. "Privacy and security in the digital age: Contemporary challenges and future directions", *The International Journal of Human Rights*, vol. 15, nº. 7, 2011, pp. 1091-1106.

HOLLIS, M.E. "Security or surveillance: Examination of CCTV camera usage in the 21st Century", *Criminology and Public Policy*, vol. 18, nº. 1, 2019, pp. 131-134.

HOPKINS, R. "An Introduction to Biometrics and Large Scale Civilian Identification", *International Review of Law, Computers & Technology*, vol. 13, nº. 3, 2010, pp. 337-363.

HOUWING, L. "Reclaim your face and the streets. Why facial recognition, and other biometric surveillance technology in public spaces, should be banned", in Quadflieg, S. et al. (Eds.), *(Dis)obedience in digital societies. Perspectives on the power of algorithms and data*, Transcript Verlag, Edinburgh, 2022, pp. 319-341.

HOWARD-HASSMAN, R.E. "Human security: Undermining human rights?", *Human Rights Quarterly*, vol. 34, 2012, pp. 88-112.

HU, M. "Biometric ID cybersurveillance", *Indiana Law Journal*, vol. 88, nº. 4, 2013, pp. 1475-1558.

HUANG, G.B. et al. "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments", *Workshop on faces in'Real-Life'Images: detection, alignment, and recognition*, 2008, pp. 1-14.

HUGHES, K. "Mass surveillance and the European Court of Human Rights", *European Human Rights Law Review*, nº. 6, 2018, pp. 589-599.

HUMBLE, K.P. "International law, surveillance and the protection of privacy", *International Journal of Human Rights*, vol. 25, nº. 1, 2021, pp. 1-25.

INIOLUWA, D.R. et al. "Saving face: Investigating the ethical concerns of facial recognition auditing", *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, pp. 145-151.

National Institute of Cybersecurity (INCIBE). *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario*, Spain, 2016.

INTRONA, L.D. & WOOD, D. "Picturing algorithmic surveillance: The politics of facial recognition systems", *Surveillance & Society*, vol. 2, nº. 2/3, 2004, pp. 177-198.

ITALIANO, G.F. et al. "L'Intelligenza Artificiale: Dalla ricerca scientifica alle sue applicazioni. Una introduzione di contesto", in PAJNO, A. et al. (Dirs.),

Intelligenza artificiale e Diritto: Una rivoluzione?, Il Mulino, Bologna, 2022, pp. 43-75.

IZQUIERDO CARRASCO, M. "La utilización policial de los sistemas de reconocimiento facial automático", *Ius et Veritas*, nº. 60, 2020, pp. 86-103.

JAIME, O. et al. "Aproximación a la seguridad nacional", in De la Corte Ibáñez, L. & Blanco Navarro, J.M. (Dirs.), *Seguridad Nacional, Amenazas y Respuestas*, Lid Editorial, Madrid, 2014, pp. 15-22.

JAIN, A.K. et al. "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, nº. 1, 2004, pp. 4-20.

JAIN, A.K. et al. "Biometrics: A tool for information security", *IEEE Transactions on Information Forensics and Security*, vol. 1, nº. 2, 2006, pp. 125-143.

JAIN, A.K. & KUMAR, A. "Biometric Recognition: An Overview", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal an Social Context*, Springer, 2012, pp. 49-77.

JANSEN, F. et al. "Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP", *Big Data & Society*, vol. 8, nº. 2, 2021, pp. 1-13.

JAR COUSELO, G. "El papel de la Policía en una sociedad democrática", *REIS. Revista Española de Investigaciones Sociológicas*, nº. 85, 1999, pp. 199-220.

JASSERAND, C.: "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data", *European Data Protection Law Review*, vol. 2, 2016, pp. 297-311.

– "Massive Facial Database and the GDPR. The New Data Protection Rules Applicable to Research", in Leenes, R. et al. (Eds.), *Data Protection and Privacy. The Internet of Bodies*, vol. I, Hart Publishing, 2018, pp. 169-188.

JENKINS, R. "Identity, surveillance and modernity", Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp.159-166.

JIA, W. et al. "A survey on dorsal hand vein biometrics", *Patern Recognition*, vol. 120, 2021, pp. 1-22.

KANADE, T. "Picture Processing System by Computer Complex and Recognition of Human Faces", *Department of Information Science*, Kyoto University, 1973.

KATROUGALOS, G. "The tension between personal freedom and security from risks", *Annuaire International des Droits de l'Homme. Conflicts de Droits de l'Homme*, vol. 4, 2009, pp. 215-221.

KAUSAR, S. et al. "Comparative study of forensic recognition and fingerprint during crime scene investigation and the role of artificial intelligence tools in forensics", *Journal of Development and Social Sciences*, vol. 5, nº. 1, 2024, pp. 585-597.

KHAIRUDDIN, A.R. et al. "A review on applied statistical and artificial intelligence techniques in crime forecasting", *IOP Conference Series: Materials Science and Engineering 551,* 2019, pp. 1-5.

KIM, H.B. et al. "Surveillance system for real-time high-precision recognition of criminal faces from wild videos" *IEEE Access,* vol. 11, 2023, pp. 56066-56082.

KIM, K.S. & JEONG, Y.H. "A Study on Crime Prediction to Reduce Crime Rate Base don Artificial Intelligence", *Korean Journal of Artificial Intelligence,* vol. 9, nº. 1, 2021, pp. 15-20.

KIND, A. "Biometrics and the metaphysics of personal identity", *IET Biometrics,* vol. 12, nº. 1, 2023, pp. 176-182.

KINDT, E.J.: *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Springer, 2013.

– "Having yes, using no? About the new legal regime for biometric data", *Computer Law & Security Review,* vol. 34, 2018, pp. 523-538.

KING, T.C. et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", *Science and Engineering Ethics,* vol. 26, nº. 89, 2020, pp. 89-120.

KIRBY, M. & SIROVICH, L. "Application of the Karhunen-Loève Procedure for the Characteriztion of Human Faces", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, nº. 1, 1990, pp. 103-108.

KLARE, B.F. et al. "Suspect Identification Based on Descriptive Facial Attributes", *IEEE International Joint Conference on Biometrics,* 2014, p. 1-8.

KOPEL, D. & KRAUSE, M. "Face the facts: facial recognition technology's troubled past-and troubling future", *Reason,* vol. 34, nº. 5, 2002.

KOSKELA, H. "'You shouldn't wear that body'. The problematic of surveillance and gender", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies,* Routledge, 2012, pp. 49-56.

KRIZHEVSKY, A. et al. "ImageNet Classification with Deep Convolutional Neural Networks", *Advances in neural information processing systems,* vol. 25, 2012, pp. 1-9.

KROENER, I. & NEYLAND, D. "New technologies, security and surveillance", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 141-148.

KUGELMANN, D. & KOSIN, C. "Surveillance powers of the police and the protection of personal data", in Alleweldt & Fickenscher (Eds.), *The police and international human rights law,* Springer, 2018, pp. 155-180.

LAUFS, J. & BORRION, H. "Technologicacl innovation in policing crime prevention: Practitioner perspectives from London", *International Journal of Police Science & Management*, vol. 24, nº. 2, 2021, pp. 190-209.

LEARNED-MILLER, E. et al. *Facial recognition technologies in the wild: A call for federal office*, MacArthur Foundation, 2020.

LEBRETON, G. "Ordre public et dignité de la personne humaine: un problème de frontière", in Redor, M.J (Dir.), *L'ordre public: Ordre publico u ordres publics? Ordre public et droits fondamentaux*, Bruylant, Bruxelles, 2001, pp. 353-367.

LECHNER, M. "Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social", *Divulgation*, vol. 1, nº. 1, 2016, pp. 1-16.

LIN, F. et al. "Super-Resolved Faces for Improved Face Recognition from Surveillance Video", in LEE, S.W. & LI, S.Z. (Eds.), *Advances in Biometrics. International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, pp. 1-10.

LIU, R. et al. "Tracking and Recognition of Multiple Faces at Distances", in LEE, S.W. & LI, S.Z. (Eds.), *Advances in Biometrics. International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, pp. 513-522.

LOCK, D. "Case Analysis. Form over substance: Human Rights Law's search for effective protections against the abuse of surveillance powers", *European Human Rights Law Review*, nº. 3, 2022, pp. 299-309.

LOMBROSO, C. *L'uomo delinquente. In rapporto all'antropologia, alla giurisprudenza ed alle discipline carcerarie*, Napoleone Editore, Roma, 1971.

LÓPEZ ORTEGA, J.J. "La protección de la intimidad en la investigación penal: necesidad y proporcionalidad de la injerencia como presupuestos de validez", in López Ortega, J.J. (Dir.), *Perfiles del derecho constitucional a la vida privada y familiar*, Consejo General del Poder Judicial, Madrid, 1996, pp. 277-307.

LOVALLO, C. "Big Brother's fall brings liberty to all: Addressing the urgency for strict regulation governing law enforcement use of facial recognition technology in Texas", *Thurgood Marshall Law Review*, vol. 46, nº. 1, 2021, pp. 67-94.

LYNCH, N. "Facial Recognition Technology in Policing and Security-Case Studies in Regulation", *Laws*, vol. 13, nº. 35, 2024, pp. 1-14.

LYON, D.: "An electronic panopticon? A sociological critique of surveillance theory", *The Sociological Review*, vol. 41, nº. 4, 1993, pp. 653-678.

– "Surveillance, security and social sorting", *International Criminal Justice Review*, vol. 17, nº. 3, 2007, pp. 161-170.

LYON, D. & WOOD, D.M. "Security, surveillance, and sociological analysis", *Canadian Review of Sociology*, vol. 49, nº. 4, 2012, pp. 317-327.

LYON, D. et al. "Introducing surveillance studies", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 1-11.

MADIEGA, T. & MILDEBRATH, H. *Regulating facial recognition in the EU*, European Parlamentary Research Service, Bruxelles, 2021.

MANN, M. & SMITH, M. "Automated Facial Recognition technology: recent developments and approaches to oversight", *University of New South Wales Law Journal*, vol. 40, nº.1, 2017, pp. 121-145.

MANTERELO, A. "The EU proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'", *Computer Law & Security Review*, vol. 29, 2013, pp. 229-235.

MANTELERO, A. & FANUCCI, F. "The international debate on AI reputation and human rights in the prism of the Council of Europe's CAHAI. Great ambitions", in Czech, P. et al. (Eds.), *European Yearbook on Human Rights 2022*, Intersentia, Cambridge, 2022, pp. 225-252.

MARÍN CASTÁN, M.L. "La dignidad humana, los Derechos Humanos y los Derechos Constitucionales", *Revista de Bioética y Derecho*, nº. 9, 2007, pp. 1-8.

MARKOWITZ, J.A. "Voice biometrics. Who are you? Your voice alone can be used to verify your personal identity –unobtrusively and invisibly", *Communication of the ACM*, vol. 43, nº. 9, 2000, pp. 66-73.

MARSHALL, J. *Personal Freedom through Human Rights Law?*, Martinus Nijhoff Publishers, Leiden, 2009.

MARSHALL, S. "Private lives and public rules", in Claes, E. et al. *Privacy and the Criminal Law*, Intersentia, Antwerpen, 2006, pp. 33-42.

MARTÍNEZ, D.E. "Beyond disciplinary enclosures: Management control in the society of control", *Critical Perspectives on Accounting*, vol. 22, 2011, pp. 200-211.

MARTÍNEZ-MORENO, P. et al. "Evidence evaluation in craniofacial superposition using likelihood ratios", *Information Fusion*, vol. 111, 2024, pp. 1-11.

MARTÍN FERNÁNDEZ, M. "Policía, profesión y organización: Hacia un modelo integral de la policía en España", *Revista Española de Investigaciones Sociológicas*, nº. 59, 1992, pp. 205-222.

MASI, I. et al. "Rapid Synthesis of Massive Face Sets for Improved Face Recognition", *12th IEEE International Conference on Automatic Face & Gesture Recognition*, 2017, pp. 604-611.

MATTA, W. "L'intelligenza artificiale per la sicurezza pubblica", in Massucci y ferrigni (Dirs.), *Per una cultura della sicurezza condivisa. Trattato di sicurezza pubblica*, Franco Angeli, Milano, 2020, pp. 283-288.

MATZNER, T. "Opening black boxes is not enough: Data-based surveillance in *Discipline and Punish* and today", *Foucault Studies*, nº. 23, 2017, pp. 27-45.

MAZUR, M. et al. "Smile photograph analysis and its connection with focal length as one of identification methods in forensic anthropology and odontology", *Forensic Science International*, vol. 335, 2022, pp. 1-9.

MEDEN, B. et al. "Privacy-Enhancing Face Biometrics: A comprehensive Survey", *IEEE Transactions on Information Forensics and Security*, vol. 16, 2021, pp. 4147-4183.

MERCADER UGUINA, J.R. "Discriminación algorítmica y derecho granular: nuevos retos para la igualdad en la era del big data", *Labos*, vol. 2, nº. 2, 2021, pp. 4-10.

MIAN, A. et al. "Keypoint Identification and Feature-Based 3D Face Recognition", in LEE, S.W., & LI, S.Z. (Eds.), *Advances in Biometrics. International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, pp. 163-171.

MILLER, K. "Total surveillance, Big data, an predictive crime surveillance: Privacy's perfect storm", *Journal of Technology Law and Policiy*, vol. 19, nº. 1, 2014, pp. 105-146.

MILOSSI, M. "Remote biometric identification systems and ethical challenges: The case of facial recognition", *21 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 2021, pp. 1-6.

MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal: Más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, nº. 20, 2018, pp. 87-130.

MITCHELL, A. "Distinguishing friend from foe: Law and policy in the age of battlefield biometrics", in *The Canadian yearbook of International Law*, vol. 50, 2012, 289-330.

MITROU, L. et al. "Perceptions of videosurveillance in Greece", in Friedewald, M. et al (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, pp. 123-138.

MORDINI, E. & MASSARI, S. "Body, biometrics and identity", *Bioethics*, vol. 22, nº. 9, 2008, pp. 488-498.

MORDINI, E. & TZOVARAS, D. (Eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012.

MORDINI, E. et al. "Introduction", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 1-19.

MOBILIO, G.: "Profilare tramite riconoscimento faciale: il caso de la sicurezza urbana", in Adinolfi, A. & Simoncini, A. (Dirs.), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizione Scientifiche Italiane, Napoli, 2022, pp. 183-202.

– "Your face is not new to me- Regulating the surveillance power of facial recognition technologies", *Internet Policy Review. Journal on Internet Regulation*, vol. 12, nº. 1, 2022, pp. 1-30.

MOFFAT, K.H. "Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates", *Theoretican Criminology*, vol. 23, nº. 4, 2019, pp. 453-470.

MOURE COLÓN, F. *Armonización de las líneas de acción de la estrategia integral de seguridad de la comunidad internacional: aportación española*, Dykinson, Madrid, 2014.

MUNARINI, M. "New perspectives on the mitigation of gender bias in AI by EU regulations", *Peace Human Rights Governance*, vol. 6, nº. 2, 2022, pp. 111-136.

MURDOCH, J. "Police powers and criminal investigations", in Alleweldt, R. & Fickenscher, G. (Eds.), *The police and international human rights law*, Springer, 2018, pp. 125-153.

MURRAY, D. "Facial recognition and the end of human rights as we know them?", *Netherlands Quarterly of Human Rights*, vol. 42, nº. 2, 2024, pp. 145-152.

MURRAY, D. & FUSSEY, P. "Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data", *Israel Law Review*, vol. 52, nº. 1, 2019, pp. 31-60.

MYTHEN, G. & WALKLATE, S. "Terrorism, Risk and International Security: The Perils of Asking: 'What if?'", *Sage Publications. Security Dialogue*, vol. 39, nº. 2-3, 2008, pp. 221-242.

NAKAR, S. & GREENBAUM, D. "Now you see me. Now you still do: Facial recognition technology and the growing of lack of privacy", *Boston University Journal of Science and Technology Law*, vol. 23, nº. 1, 2017, pp. 88-122.

NERONI REZENDE, I.: "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective", *New Journal of European Criminal Law*, vol. 11, nº. 3, 2020, pp. 375-389.

– *Surveillance Risks in IoT applied to Smart cities*, Tesis doctoral defendida en 2023 en la Universidad de Bolonia, Italia.

NIKLAS, P. & BARRERA, G. "Biometría aplicada a la seguridad pública", *Simposio Argentino sobre Tecnología y Sociedad (STS)-JAIIO 46*, 2017, pp. 146-160.

NINAQUISPE SOTO, M.E. et al. "Technology and crime prevention: A systematic review of literatura", *2021 Fifth World Conference on Smat Trends in Systems Security and Sustainabiligy (WorldS4)*, IEEE, 2021, pp. 257-283.

NISSENBAUM, H. "protecting privacy in an inforamtion age: the problem of privacy in public", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, pp. 177-214.

NIXON, M.S. et al. "On soft biometrics", *Pattern Recognition Letters*, vol. 68, 2015, pp. 218-230.

NORTH-SAMARDZIC, A. "Biometric technology and ethics: Beyond security applications", *Journal of Business Ethics*, vol. 167, nº. 3, 2020, pp. 433-450.

NOVELLI, C. *AI and legal personhood: a theoretical survey*, Tesis Doctoral defendida en la Universidad de Bolonia, Italia, 2022.

NOVOKMET, A. et al. "Facial recognition technology in EU criminal justice-human rights implications and challenges", *Digitalization and Green Transformation of the EU*, vol. 7, 2023, pp. 525-570.

Observatorio de la Seguridad de la Información. *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*, Ministerio de Industria, Turismo y Comercio, Spain, 2011.

ODDENINO, A. "Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 165-201.

O'LEARY, S. "La surveillance de masse et la Convention Européenne des Droits de l'Homme", in Lemmens, K. et al (Eds.), *Human Rights with a Human Touch. Liber amicorum Paul Lemmens*, Intersentia, Cambridge, 2019, pp. 253-279.

ORIT, K. *In the face of ethics police use of live facial recognition technology*. Thesis submitted for the degree of Doctor of Philosophy (PhD) in Law, London, May 2024.

ORTEGA ANDEREZ, D. et al. "The rise of technology in crime prevention: opportunities, challenges and practitioners' perspectives", *arXiv preprint: 2102.04204*, 2021, pp. 1-19.

ORWELL, G. *1984*, Penguin Random House Grupo Editorial, 24ª reimpresión, 2023.

PALMA ORTIGOSA, A. "El ciclo de vida de los sistemas de Inteligencia Artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos", in Cotino Hueso (Dir.), *Derechos y garantías ante la Inteligencia Artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, pp. 29-51.

PANKANTI, S. BOLLE, R.M. & JAIN, A. "Biometrics: The Future of Identification [guest editors' introduction]", *Computer*, vol. 33, nº. 2, 2000, pp. 46-49.

PAREJO ALFONSO, L. "El derecho fundamental a la intimidad y sus restricciones", in López Ortega, J.J. (Dir.), *Perfiles del derecho constitucional a la vida privada y familiar*, Consejo General del Poder Judicial, Madrid, 1996, pp.13-48.

PARK, U. & JAIN, A.K. "3D Model-Based Face Recognition in Video", in Lee, S.W., & Li, S.Z. (Eds.), *Advances in Biometrics International Conference ICB 2007, International Conference, ICB 2007. Seoul, Korea*, Springer, 2007, pp. 1085-1094.

PAVIA, M.L. "La dignité de la personne humaine", in Cabrillac, R. et al. (Dirs.), *Libertés et droits fondamentaux*, Dalloz, Paris, 2007, pp. 145-164.

PELAIA, C. & NUCERA, G.G. "La prassi del *racial profiling* in Europa: Una forma di discriminazione istituzionale", *I Diritti dell'Uomo*, vol. 27, nº. 1, 2016, pp. 79-106.

PENNEY, J.W. "Chilling effects: Online surveillance and Wikipedia use", *Berkeley Tech. LJ.*, vol. 31, 2016, pp. 117-182.

PÉREZ TRENCH, N. "Los sistemas de reconocimiento facial: Una mirada a la luz del examen de proporcionalidad", *Revista Internacional de Derechos Humanos*, vol. 12, nº. 1, 2022, pp. 55-88.

PÉREZ Y MADRID, A. *El reconocimiento facial es un superpoder. Cómo te afectará y por qué deberías conocerlo*, Dykinson, Madrid, 2021.

PHILIPPE, X. "La liberté d'aller et de venir", in Cabrillac, R. et al. (Dirs.), *Libertés et droits fondamentaux*, Dalloz, Paris, 2007, pp. 319-340.

PISTILLI, C. "L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine: tra prospettive di sviluppo ed esigenze di coordinamento", in Balbi, G. et al, (Dirs.), *Diritto penale e intelligenza artificiale "nuovi scenari",* G. Giappichelli Editore, Torino, 2022, pp. 145-166.

PIZA, E.L. et al. "CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis", *Criminology and Public Policy*", vol. 18, nº. 1, 2019, pp. 135-159.

PLACCO, A.V. "La protection des données à caractère personnel dans le cadre de la jurisprudence de la Cour de Justice de l'Union Euorpéenne relative aux droits fondamentaux", in Grosjean, A. (Dir.), *Enjeux européennes et mondiaux de la protection des données personnelles*, Larcier, Bruxelles, 2015, pp. 27-51.

PORCEDDA, M.G. "On boundaries-Finding the essence of the right to the protection of personal data", in Leenes, R. et al. (Eds.), *Data Protection and Privacy. The Internet of Bodies*, vol. I, Hart Publishing, 2018, pp. 277-312.

PRABHAKAR, S. et al. "Biometric recognition: Security and privacy concerns", *IEEE Security and Privacy*, vol. 1, nº. 2, 2003, pp. 33-42.

PRESNO LINERA, M.A. *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid, 2022.

PREST, E.M. *Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System*, Federal Bureau of Investigation, 2019.

PURSHOUSE, J. & CAMPBELL, L. "Automated facial recognition and policing: A *Bridge* too far?", *Legal Studies*, vol. 42, 2022, pp. 209-227.

QIAN, Y. et al. "Task Specific Networks for Identity and Face Variation", *13th IEEE International Conference on Automatic Face on Automatic Face & Gesture Recognition*, 2018, pp. 271-277.

RACHELS, J. "Why privacy is important", in Barendt, E. (Ed.), *Privacy*, Ashgate, Dartmouth, 2001, pp.11-21.

RAFFIOTA, E.C. & BARONI, M. "Intelligenza artificiale, strumenti di identificazione e tutela dell'identità", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 363-387.

RAI, A. "Explanaible AI: From black box to glass box", *Journal of the Academy of Marketing Science*, vol. 48, 2020, pp. 137-141.

RAJ, P. et al. "Facial recognition system for identification of missing person", *Kalpa Publications in Computing*, vol. 19, 2024, pp. 322-332.

RAJI, I.D. et al. "Saving Face: Investigating the Ethical Concerns of Facil Recognition Auditing", *Proceedings of the AAAI/ACM Conference on AI, Ethics and Society*, 2020, pp. 145-151.

RAPOSO, V.L.: "The use of facial recognition technology by law enforcement in Europe: a Non-Orwellian Draft Proposal", *European Journal on Criminal Policy and Research*, vol. 29, nº. 4, 2021, pp. 515-533.

- "Health, privacy and liberty: a call for digital governance during (and after) the pandemic", *The International Journal of Human Rights*, vol. 27, nº. 3, 2023, pp. 529-551.
- "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", *Information & Communications Technology Law*, vol. 32, nº. 1, 2023, pp. 45-63.

RATHA, N.K. et al. "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, vol. 40, nº. 3, 2001, pp. 614-634.

RENUCCI, J.F. "Surveillance de masse et Convention Européenne des Droits de l'Homme", *Recueil Dalloz*, nº. 3, 2019, pp. 151-156.

REDDICK, C.G. et al. "Public opinion on National Security Agency surveillance multi-method approach", *Government Information Quarterly*, vol. 32, 2015, pp. 129-141.

REDING, V. "Foreword. Privacy Implications of Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. V-VI.

RENGEL, A. *Privacy in the 21st Century*, Martinus Nijhoff Publishers, Leiden, 2013.

RICCIO, G.M. & GIANNONE CODIGLIONE, G. "La rilevanza delle basi giuridiche per il trattamento di dati personali mediante sistemi di intelligenza artificiale", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 281-311.

RIERA, A. et al. "Electrophysiological Biometrics: Opportunities and Risks", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 149-176.

RIESGO GARCÍA, M. "Inteligencia Artificial. Enfoque policial", en Peralta, Salvador Torres y Herrera (Coords.), *El Derecho y la Inteligencia Artificial*, Editorial Universidad de Granada, Granada, 2022, pp. 483-488.

RUSINOVA, V. "Privacy and the legalisation of mass surveillance: In search of a second wind for international human rights law", *The International Journal of Human Rights*, vol. 26, nº. 4, 2022, pp. 741-756.

SAINI, M. & KAPOOR, A.K. "Biometrics in Forensic Identification: Applications and Challenges", *Journal of Forensic Medicine*, vol. 1, nº. 1, 2016, pp. 1-6.

SAKAI, T. et al. "Picture Processing System Using a Computer Complex", *Computer Graphics and Image Processing*, vol. 3, 1973, pp. 207-215.

SALAZAR, I. "El diseño ético de la inteligencia artificial para no discriminar ni lesionar derechos", in Balaguer Callejón, F. & Cotino Hueso, L. (Dirs.), *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, pp. 85-110.

SANABRIA MOYANO, J.E. et al. "Tecnología de reconocimiento facial y sus riesgos en los derechos humanos", *Revista Criminalidad*, vol. 64, nº. 3, 2022, pp. 61-78.

SANDHYA, S. et al. "Deep Learning based face detection and identification of criminal suspects", *Computers, Materials & Continua*, vol. 74, nº. 2, 2023, pp. 2331-2343.

SAN MARTÍN CASTRO, C. "La privación de la libertad personal en el proceso penal y el Derecho Internacional de los Derechos Humanos", *Derecho y Sociedad*, nº. 20, 2003, pp. 160-173.

SANSÓ-RUBERT, D. & GIMÉNEZ-SALINAS FRAMIS, A., "Crimen organizado", in De la Corte Ibáñez, L. & Blanco Navarro, J.M. (Dirs.), *Seguridad Nacional, Amenazas y Respuestas*, Lid Editorial, Madrid, 2014, pp. 133-148.

SANSÓ-RUBERT PASCUAL, D. "Inteligencia artificial al servicio de la criminalidad organizada ¿Mito o realidad?", *Revista Ábaco*, vol. 1, nº. 103, 2020, pp. 128-138.

SANTAMARIA, K.Y. "Facial recognition technology and law enforcement: Select constitutional considerations", *Congressional Research Service*, 2020.

SARTOR, G. *L'intelligenza Artificiale e il Diritto*, Giappichelli, Torino, 2022.

SCHEPISI, C. "Diritti fondamentali, principi democratici e *rule of law*: quale ruolo e quale responsabilità per gli stati nella regolazione dell'intelligenza artificiale", in PAJNO, A. et al. (Dirs.), *Intelligenza artificiale e Diritto: Una rivoluzione?*, Il Mulino, Bologna, 2022, pp. 203-237.

SCHUETZ, P.N.K. "Fly in the face of bias: Algorithmic bias in law enforcement's facial recognition technology and the need for an adaptative legal framework", *Minnesota Journal of Law,* vol. 39, nº. 1, 2021, pp. 221-254.

SERRATOSA, F. *La biometría para la identificación de personas*, Universitat Oberta de Catalunya, Barcelona, 2008.

SEECAMP, A. & SÖFFNER, J. "A Postscript to the 'Postscript on the societies of control'", *SubStance*, vol. 53, nº. 2, 2024, pp. 75-85.

SHARIF, M. et al. "An Overview of Biometrics Methods", in Singh, A.K., & Mohan, A. (Eds.), *Handbook of Multimedia Information Security: Techniques and Applications*, Springer, 2019, pp. 15-35.

SHIWAKOTI, N. et al. "Exploring Jaywalking and Intersections", *39th Australasian transport research fórum*, Auckland, New Zeland, 2017, pp. 1-9.

SHREYA, S. & CHATTERJEE, K. "Latent fingerprint and Iris fusion for enhancement of performance identification system", *Expert Systems With Applications*, vol. 235, 2024, pp. 1-15.

SIEBER, U. "The paradigm shift in the global risk society: from criminal law to global security law – an analysis of the changing limits of crime control", *Journal of Eastern European Criminal Law*, nº. 1, 2016, pp. 14-27.

SIEGERT, K. "The police and the human right to peaceful assembly", in Alleweldt & Fickenscher (Eds.), *The police and international human rights law*, Springer, 2018, p. 217-243.

SILVA, I. et al. "Using micro-services and artificial intelligence to analyze images in criminal evidences", *Forensic Science International: Digital Investigation*, nº. 37, 2021, pp. 1-9.

SIMÓN CASTELLANO, P. "Allende una teoría general de las garantías para una inteligencia artificial confiable", in Balaguer Callejón, F. & Cotino Hueso, L. (Dirs.), *Derecho público de la inteligencia artificial*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023, pp. 111-148.

SINGH, R. et al. "Implementation of iris recognition as a security measure against cyber crime in hyperledger fabric", *Semiconductor Optoelectronics*, vol. 41, nº. 11, 2022, pp. 441-452.

SIROVICH, L. & KIRBY, M. "Low-dimensional procedure for the characterization of human faces", *Optical Society of America*, vol. 4, nº. 3, 1987, pp. 519-524.

SKOGAN, W.G. "The future of CCTV", *Criminology and Public Policy*, vol. 18, nº. 1, 2019, pp. 161-166.

SLOBOGIN, C. & BRAYNE, S. "Surveillance technologies and Constitutional Law", *Annual Review of Criminology*, vol. 6, 2023, pp. 219-240.

SMITH, M. & MILLER, S. *Biometric identification, Law and Ethics*, Springer, 2021.

SORIANO ARNANZ, A. "Discriminación algorítmica: Garantías y protección jurídica", in Cotino Hueso, L. (Dir.), *Derecho y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Navarra, 2022, pp. 139-169.

SORIANO MORENO, S. "Las reformas legislativas en los Estados miembros de la Unión Europea frente al terrorismo: análisis desde los derechos fundamentales", in Godoy, O. (Coord.), *Libertad y Seguridad en un contexto global. Retos y desafíos para los sistemas de garantía de los derechos fundamentales*, Dykinson, Madrid, 2020, pp. 81-111.

SPAEMANN, R. "Sobre el concepto de dignidad humana", *Persona y Derecho*, nº. 19, 1988, pp. 13-33.

SPROKKEREEF, A. & HERT, P. "Biometrics, Privacy and Agency", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 81-101.

STITILIS, D. & LAURINAITIS, M. "Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law", *Computer Law & Security Review*, vol. 33, 2017, pp. 618-628.

STONE, C.A. & ZISSU, A. "Registered Traveler Program: The Financial Value of Registering the Good Guys", *Review of Policy Research*, vol. 24, nº. 5, 2007, pp. 443-462.

STRAUß, S. "A game of hide-and-seek? Unscrambling the trade-off between privacy and security", in Friedewald, M. et al (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, pp. 255-272.

SUMER, B. "When do the images of biometric characteristics qualify as special categories of data under the GDPR?: A systematic approach to biometric data processing", *2022 Intenational Conference of the Biometrics Special Interest Group (BIOSIG)*, 2022, pp. 1-6.

SUSI, M. "The right to be forgotten", in Von Arnauld, A. et al. (Eds.), *The Cambridge Handbook of new human rights. Recognition, novelty, rhetoric,* Cambridge University Press, Cambridge, 2020, pp. 287-307.

TAIGMAN, Y. et al. "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, pp. 1701-1708.

TAMBOU, O. "À la recherche d'un regime coherent de protection des données personnelles contre les mesures de surveillance étatique. CJUE, 16 juillet 2020, *Facebook Ireland et Schrems,* aff. C-311/18 (affaire dite *Schrems 2*) ; CJUE, 6 octobre 2020, *La Quadrature du Net,* affaires jointes C-511/18 et C-512/18 ; *Ordre des barreaux francophones et germanophones,* aff. C-520/18 ; CJUE, 6 octobre 2020, *Privacy International*, aff. C-623/17", *Annuaire Française de Droit International*, CNRS Éditions, Paris, 2020, pp. 595-606.

TASKIRAN, M. et al. "Face recognition: Past, present and future (a review)", *Digital Signal Processing*, vol. 106, 2020, pp. 1-28.

TASSONE, L. "La protection des données dans la jurisprudence de la Cour Européenne des Droits de l'Homme", in Grosjean, A. (Dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, Bruxelles, 2015, pp. 53-70.

TAVAREZ-ALVARADO, H.A. et al. "Factores de riesgo en la violación de derechos humanos por parte de policías", *Ratio Juris*, vol. 19, nº. 38, 2024, pp. 1-12.

TERWANGNE, C. "L'illégalité nuancée de la surveillance numérique: La réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de Justice de l'Union Européenne", *Revue Trimestrielle des Droits de l'Homme*, nº. 129, 2022, pp. 3-27.

TINOCO PASTRANA, A. "La modernización de la cooperación judicial transfronteriza en la Unión Europea: la implementación de la digitalización", *Revista Asociación de Profesores de Derecho Procesal de las Universidades Españolas*, nº. 8, 2023, pp. 109-151.

THOMPSON, K.A. "Countenancing employment discrimination: Facial recognition in background checks", *Texas A&M Law Review*, vol. 8, nº. 1, 2020, pp. 63-88.

THYS, S. VAN RANST-W. & GOEDEMÉ, T. "Fooling automated surveillance cameras: Adversarial patches to attack person detection", *arXiv.org,* (Institutional Repository of the University of Cornell), New York, 2019.

TORRE, M. "Nuove tecnologie e trattamento dei dati boimetrici nel proceso penale: il sistema automatico di riconoscimento delle imagini", in Adinolfi, A. & Simoncini, A. (Dirs.), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizione Scientifiche Italiane, Napoli, 2022, pp. 679-695.

TORRES LÓPEZ, L.S. & PERALTA GUTIÉRREZ, A. "Uso policial de sistemas de inteligencia artificial en el ámbito comparado", in Peralta et al. (Coords.), *El Derecho y la Inteligencia Artificial*, EUG, Granada, 2022, pp. 453-481.

TSCHIDER, C.A. "Beyond de 'black box'", *Denver Law Review*, vol. 98, nº. 3, 2021, pp. 683-724.

TURK, M. & PENTLAND, A. "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, vol. 3, nº. 1, 1991, pp. 71-86.

VALLS PRIETO, J.: *Inteligencia artificial, Derechos Humanos y bienes jurídicos*, Aranzadi, Navarra, 2021.

- "Sobre la responsabilidad penal por la utilización de sistemas inteligentes", *Revista Electrónica de Ciencia Penal y Criminología*, vol. 24, nº. 27, 2022, pp. 1-35.
- "Derecho penal y la inteligencia artificial: Una metodología de análisis", in en Peralta et al. (Coords.), *El Derecho y la Inteligencia Artificial*, EUG, Granada, 2022, pp.489-511.

VAN DER PLOEG, I.: Van DER PLOEG, I. "The body as data in the age of information", in Ball, K. et al. (Eds.), *Routledge Handbook of Surveillance Studies*, Routledge, 2012, pp. 176-183.

- "Security in the Danger Zone: Normative Issues of Next Generation Biometrics", in Mordini, E. & Tzovaras, D. (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp. 287-303.

VERMEERSCH, H. & DE PAUW, E. "The acceptance of new security oriented technologies", in Friedewald, M. et al (Eds.), *Surveillance, privacy and security. Citizens' perspectives*, Routledge, 2017, pp. 52-70.

VAN EIJK, N. "Mass collection of data: failing typologies", in *Human rights challenges in the digital age: Judicial perspectives*, Council of Europe. European Court of Human Rights, Strasbourg, 2020, pp. 167-172.

WACHTER, S. "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What this means for the European Union, the United States, and beyond", *Yale Journal of Law & Technology, Special Issue: Yale Information Society Project Digital Public Sphere Series*, vol. 26, nº. 3, 2024, pp. 671-718.

WANG, M. & DENG, W. "Deep face recognition: A survey", *Neurocomputing*, vol. 429, 2021, pp. 215-244.

WANG, H. & MA, S. "Preventing crimes against public health with artificial intelligence and machine learning capabilities", *Socio-Economic Planning Sciences*, nº. 80, 2022, pp. 1-8.

WANG, Q. et al. "CSAN: A neural network benchmark model for crime forecasting in spatio-temporal scale", *Knowledge-Based Systems*, nº. 189, 2020, pp. 1-16.

WANG, V. & TUCKER, J.V. "I am not a number': Conceptualising identity in digital surveillance", *Technology in Society*, vol. 67, 2021, pp. 1-8.

WAYMAN, J.L. "The scientific development of biometrics over the last 40 years", *The History of Information Security: A Comprehensive Handbook*, Elsevier Science B.V., 2007, pp. 263-274.

WOODWARD, J.D. *Super Bowl surveillance. Facing up to biometrics*, RAND Arroyo Center, 2001.

XENOS, D. "The protection against crime as a human right: positive obligations of the police", in Alleweldt & Fickenscher (Eds.), *The police and international human rights law*, Springer, 2018, pp. 181-215.

XIE, S. & TU, Z. "Holistically-Nested Edge Detection", *Proceedings of the IEEE International Conference on Computer Vision*, 2015, pp. 1395-1403.

YANG, J. et al. "Weakly-supervised Disentangling with Recurrent Transformations for 3D View Synthesis", *Advances in neural information processing systems*, vol. 28, 2015, pp. 1-9.

YUDKIVSKA, G. "New approach to the right to privacy in times of transparency and mass surveillance", in Sturma, P. et al (Eds.), *70th Anniversary of the European Convention on Human Rights*, Rw&w Science & New Media, Bayern, 2021, pp. 47-60.

YUE LIU, N. *Bio-Privacy. Privacy Regulations and the Challenge of Biometrics*, Routledge, Oxon, Abingdon, 2012.

ZALNIERIUTE, M. "Glukhin v. Russia. App. Nº. 11519/20. Judgment", *American Journal of International Law*, vol. 117, nº. 4, 2023, pp. 695-701.

ZAVRSNIK, A. "Criminal justice, artificial intelligence systems, and human rights", *ERA Forum*, vol. 20, 2020, pp. 567-583.

ZOUAVE, E. & SCHROERS, J. "You've been measured, you've been weighed and you've been found suspicious. Biometrics and data protection in criminal justice processing", in Leenes, R. et al. (Dirs.), *Data protection and privacy. The internet of bodies, vol. II*, Hart Publishing, 2018, pp. 1-19.

ZUIDERVEEN BORGESIUS, F.J. "Strengthening legal protection against discrimination by algorithms and artificial intelligence", *The International Journal of Human Rights*, vol. 24, nº. 10, 2020, pp. 1572-1593.

ZUREIK, E. & HINDLE, K. "Governance, security and technology: the case of biometrics", *Studies in Political Economics*, vol. 73, nº. 1, 2004, pp. 113-137.

WEBGRAPHY

AI HLEG. *A definition of AI: main capabilities and disciplines*, European Commission, 2019. Electronic resource obtained via the Web: https://ec.europa.eu/digital-inglemarket/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines. [Retrieved on 2 November, 2023].

ALMOGUERA, P. "Singapur estrena un sistema de verificación facial como DNI", *El País*, 20 de octubre de 2020. Electronic resource obtained via the Web: https://elpais.com/retina/2020/10/02/innovacion/1601653052_245522.html, [retrieved on 2 April, 2024].

ANNAN, K. '*Nosotros los Pueblos'. La función de las Naciones Unidas en el siglo XXI*, Cumbre del Milenio de las Naciones Unidas, 2000. Electronic resource obtained via the Web: https://www.un.org/es/events/pastevents/millennium_summit/sg_report/full.htm, [retrieved on 20 December, 2023].

ASOCIACIÓN POR EL AVANCE DE LA INTELIGENCIA ARTIFICIAL. *Artificial Intelligence and Life in 2030*, 2016. Recurso electrónico obtenido de la Web: https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, [retrieved on 2 November, 2023].

ATICK, J. "Biometrics. 10 Breakthrough technologies 2001", *MIT Technology Review*, 2001. Electronic resource obtained via the Web: https://www.technologyreview.com/10-breakthrough-technologies/2001/, [retrieved on 21 August, 2024].

Aurora-AI. Electronic resource obtained via the Web: https://aurora-ai.com/, [retrieved on 10 March, 2024].

Autoridad Sueca para la protección de la privacidad, 10 de febrero de 2021, DI-2020-2719. Electronic resource obtained via the Web: https://gdprhub.eu/index.php?title=IMY_(Sweden)_-_DI-2020-2719, [retrieved on 3 April, 2024].

BBC: BBC, *Chinese AI caught out by face in bus ad*, 27 November 2018. Electronic resource obtained via the Web: https://www.bbc.com/news/technology-46357004, [retrieved on 28 July, 2024].

– *Twitter demands AI company stops 'collecting faces'*, 23 de enero de 2020. Electronic resource obtained via the Web: https://www.bbc.com/news/technology-51220654, [retrieved on 18 July, 2024].

BRACERO, F. "Una web facilita identificar a 6.000 de los asaltantes al Capitolio", *La Vanguardia*, 25 January 2021. Electronic resource obtained via the Web: https://www.lavanguardia.com/tecnologia/20210125/6196390/web-facilita-identificar-6-000-asaltantes-capitolio.html, [retrieved on 11 September, 2024].

BURT, C. "Facial recognition temperature scanning, wearables and voice biometrics deployed for COVID-10 spread prevention", *Biometric update*, 3 August 2020. Electronic resource obtained via the Web: https://www.biometricupdate.com/202008/facial-recognition-temperature-scanning-wearables-and-voice-biometrics-deployed-for-covid-19-spread-prevention, [retrieved on 15 August, 2024].

CAMPBELL, F. "Data Scraping-Considering the Privacy Issues", *Fieldfisher*, 2019. Electronic resource obtained via the Web: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues, [retrieved on 18 July, 2024].

CHERRADÍ, A. "Reconocimiento facial mediante PCA frente a aprendizaje profundo", *Medium*, 2020. Electronic resource obtained via the Web: https://towardsdatascience.com/face-recognition-using-deep-learning-b9be73689a23, [retrieved on 6 November, 2023].

CHRISTAKIS, T. BECUYWE, M. & AI-REGULATION TEAM. *Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021*, AI-Regulation.com, May 27th, 2021. Electronic resource obtained via the Web: https://ai-regulation.com/facial-recognition-inthe-draft-european-ai-regulation-final-report-on-thehigh-level-workshop-held-on-april-26-2021/, [retrieved on 7 May, 2024].

CLAYTON, J. "La controvertida tecnología que usa Ucrania para identificar a los muertos y enemigos en la guerra", *BBC News*, 3 de abril de 2022. Recurso electrónico obtenido a travé de la Web: https://www.bbc.com/mundo/noticias-internacional-61096583, [retrieved on 18 July, 2024].

COLLINS, J. "China is using facial recognition to track millions of Muslim citizens wherever they go", *Quartz*, 17 de febrero de 2019. Recurso electrónico obtenido a través de la Web: https://qz.com/1552708/china-is-using-facial-recognition-to-track-millions-of-muslim-citizens-wherever-they-go/, [retrieved on 11 March, 2024].

COMUNICACIÓN PODER JUDICIAL, *La Audiencia Nacional absuelve a un joven británico juzgado por enviar un mensaje durante un vuelo en el que amenazaba con volar el avión*, 25 January 2024. Electronic resource obtained via the Web: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-absuelve-a-un-joven-britanico-juzgado-por-enviar-un-

mensaje-durante-un-vuelo-en-el-que-amenazaba-con-volar-el-avion-, [retrieved on 28 August, 2024].

CRUZ ROJA. *Cruz Roja trabaja en un software de reconocimiento facial que ayude a localizar migrantes desaparecidos*, 28 August 2024. Electronic resource obtained via the Web: https://www2.cruzroja.es/-/cruz-roja-trabaja-en-un-software-de-reconocimiento-facial-que-ayude-a-localizar-migrantes-desaparecidos, [retrieved on 29 August, 2024].

DE LA MATA BARRANCO, N.J. "Inteligencia artificial autónoma y responsabilidad penal de las personas jurídicas", *Almacén de Derecho*. Electronic resource obtained via the Web: https://almacendederecho.org/inteligencia-artificial-autonoma-y-responsabilidad-penal-de-las-personas-juridicas, [retrieved on 26 January, 2024].

DÍAZ, M.P. "Vueling implanta el reconocimiento facial para embarcar en avión: así funciona y a quién se envían tus datos", *El Confidencial*, 19 January, 2024. Electronic resource obtained via the Web: https://www.elconfidencial.com/tecnologia/2024-01-19/vueling-implanta-reconocimiento-facial-viajes_3814339/, [retrieved on 10 August, 2024].

EDPB. *Swedish DPA: Police unlawfully used facial recognition app*, 12 de febrero de 2021. Electronic resource obtained via the Web: https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en, [retrieved on 21 July, 2024].

EUROPAPRESS. "Amazon extiende su prohibición de usar su reconocimiento facial para fines policiales de forma indefinida", 19 de mayo de 2021. Electronic resource obtained via the Web: https://www.europapress.es/portaltic/empresas/noticia-amazon-extiende-prohibicion-usar-reconocimiento-facial-fines-policiales-forma-indefinida-20210519121835.html, [retrieved on 10 June, 2024].

EUROPEAN DATA PROTECTION SUPERVISOR. *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*. Electronic resource obtained via the Web: https://www.edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en, [retrieved on 8 May, 2024].

FUNDACIÓN ÉTICAS. *Auditoría Externa del Sistema VioGén*, 2022. Electronic resource obtained via the Web: https://eticasfoundation.org/wp-content/uploads/2022/04/ETICAS-_-Auditori%CC%81a-Externa-del-sistema-VioGe%CC%81n-_-20220308.docx.pdf. [Retrieved on 18 March, 2024].

HEDGECOE, G. "El escándalo en un pequeño pueblo de España por las imágenes de decenas de niñas y jóvenes desnudas generadas por IA", *BBC News*, 25 de septiembre de 2023. Electronic resource obtained via the Web:

https://www.bbc.com/mundo/articles/cz9r6792k13o, [retrieved on 7 February, 2024].

HERNÁNDEZ, J. "Lo que se sabe del atentado mortal en Solingen (Alemania) durante la celebración de un festival", *Huffpost*, 24 August 2024. Electronic resource obtained via the Web: https://www.huffingtonpost.es/global/lo-atentado-mortal-solingen-alemania-celebracion-festival.html, [retrieved on 31 August, 2024].

INTERPOL. *Reconocimiento facial*. Electronic resource obtained via the Web: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial, [retrieved on 29 August, 2024].

JAKHAR, P. "Coronavirus: las innovadoras tecnologías que está utilizando China para combatir la COVID-19 (y las preocupaciones que plantean), *BBC*, 4 de marzo de 2020. Electronic resource obtained via the Web: https://www.bbc.com/mundo/noticias-51736635, [retrieved on 28 July, 2024].

KAI YI, W. "No need to scan Passport for immigration clearance at Changi Airport's T4 in contactless trial", *The Straits Times*, 4 de diciembre de 2019. Electronic resource obtained via the Web: https://www.straitstimes.com/singapore/transport/contactless-immigration-trial-extended-to-changi-airport-t4, [retrieved on 2 April, 2024].

KIND, C. "Containing the canary in the AI coalmine-the EU's efforts to regulate biometrics. Exploring the gaps and risks relating to biometrics in the EU's draft AI regulation", *Ada Lovelace Institute*. Electronic resource obtained via the Web: https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/, [retrieved on 8 May, 2024].

LABORDE, A. "Detenido injustamente un afroamericano en EE UU por un error en el sistema de reconocimiento facial", *El País*, 26 June 2020. Electronic resource obtained via the Web: https://elpais.com/tecnologia/2020-06-26/un-afroamericano-es-detenido-injustamente-por-un-error-en-el-sistema-de-reconocimiento-facial.html, [retrieved on 1 August, 2024].

LA VANGUARDIA. "Comunicado: reconocimiento facial en el fútbol uruguayo", 26 de abril de 2018. Electronic resource obtained via the Web: https://www.lavanguardia.com/vida/20180426/443015024931/comunicado-reconocimiento-facial-en-el-futbol-uruguayo.html, [retrieved on 10 March, 2024].

MERINO, M. "Estos son los métodos con los que intentan sortear el reconocimiento facial los defensores de la privacidad", *Xataka*, 10 April 2019. Recurso electrónico obtenido de la Web: https://www.xataka.com/inteligencia-artificial/estos-metodos-que-intentan-sortear-reconocimiento-facial-defensores-privacidad, [retrieved on 2 August, 2024].

MINISTERIO DEL INTERIOR. *Informe Anual. Personas desaparecidas durante el año 2023*, 2024. Electronic resource obtained via the Web: www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2024/informe_2024-ACCESIBLE.pdf, [retrieved on 29 August, 2024].

MIRANDA, B. "Julian Assange: así fue la gran filtración de documentos clasificados en 2010 por la que EE.UU. pide la extradición del fundador de Wikileaks", *BBC News*, 12 de abril de 2019. Electronic resource obtained via the Web: https://www.bbc.com/mundo/noticias-internacional-47902652, [retrieved on 8 February, 2024].

NARANJO, J.C. "Reconocimiento facial, ¿el fin de la violencia en los estadios de fútbol?", *Crónica de Deportes*, 1 de mayo de 2018. Electronic resource obtained via the Web: https://cronicaglobal.elespanol.com/deportes/reconocimiento-facial-violencia-estadios-futbol_138041_102.html, [retrieved on 10 March, 2024].

NAVARRO, B. "IBM y Amazon abjuran de la tecnología de reconocimiento facial por su sesgo racista", *La Vanguardia*, 16 June 2020. Electronic resource obtained via the Web: https://www.lavanguardia.com/internacional/20200611/481710398480/ibm-reconocimiento-facial-racismo-tecnologia-negros.html, [retrieved on 2 August, 2024].

PASCUAL, M.G. "La policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial", *El País*, 28 May 2024. Electronic resource obtained via the Web: https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html, [retrieved on 10 August, 2024].

PESENTI, J. *Facebook. Una actualización a nuestro uso del reconocimiento facial*, 2021. Electronic resource obtained via the Web: https://about.fb.com/ltam/news/2021/11/una-actualizacion-a-nuestro-uso-del-reconocimiento-facial/, [retrieved on 18 July, 2024].

Predpol. Electronic resource obtained via the Web: https://www.predpol.com/, [retrieved on 19 December, 2023].

PRIVACY INTERNATIONAL, *Bulk powers in the investigatory powers bill: The question of trust remains unanswered*, 2016. Electronic resource obtained via the Web: https://www.politico.eu/wp-content/uploads/2016/09/PI_Lords.pdf, [retrieved on 2 September, 2024].

ROSENBERG, M. et al. "La empresa que explotó millones de datos de usuarios de Facebook", *The New York Times*, 20 de marzo de 2018. Electronic resource obtained via the Web: https://www.nytimes.com/es/2018/03/20/espanol/cambridge-analytica-facebook.html, [retrieved on 18 July, 2024].

SÁNCHEZ, J. "IBM abandona el mercado de reconocimiento facial por preocupaciones sobre sesgos raciales", ABC, 9 de junio de 2020. Electronic resource obtained via the Web: https://www.abc.es/tecnologia/informatica/soluciones/abci-injusticia-y-sesgos-reconocimiento-facial-debate-abre-despues-abandono-esta-tecnologia-202006091502_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ftecnologia%2Finformatica%2Fsoluciones%2Fabci-injusticia-y-sesgos-reconocimiento-facial-debate-abre-despues-abandono-esta-tecnologia-202006091502_noticia.html, [retrieved on 10 June, 2024].

SANER, E. "Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in box'", *The Guardian*, 31 de enero de 2024. Electronic resource obtained via the Web: https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box, [retrieved on 7 February, 2024].

SCHRÖDER, A. "'Real-time' versus 'post'biometric identification systems under the AI Act", *ALTI Forum*, 14 de octubre de 2022. Electronic resource obtained via the Web: https://alti.amsterdam/schroder-biometric/, [retrieved on 22 de mayo de 2024].

SDPA. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020. Electronic resource obtained via the Web: https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf. [Retrieved on 7 November, 2023].

VIDAL LIY, M. "2,5 millones de personas en China, bajo el control de una empresa de vigilancia facial", *El País*, 18 de febrero de 2019. Electronic resource obtained via the Web: https://elpais.com/internacional/2019/02/17/actualidad/1550422679_515333.html, [retrieved on 11 March, 2024].

LEGISLATION

International

Universal Declaration of Human Rights adopted and proclaimed by the United Nations General Assembly in its resolution 217 A (III) of 10 December 1948.

International Covenant on Civil and Political Rights adopted and opened for signature, ratification and accession by General Assembly of the United Nations in its resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49.

Europe

European Convention on Human Rights, Rome, 4 November 1950.

Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on May 2018. Convention 108+ [COM(2018) 451 final].

European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018).

White paper on artificial intelligence. A European approach to excellence and trust. COM(2020) 65 final.

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, nº. 225, 5 September 2024.

European Union

Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995. On the protectioni of individuals with regard to the processing of personal data and on the free movement of such data.

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

Charter of fundamental rights of the European Union (2000/C 364/01).

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013, on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

European Parliament Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the pólice and judicial authorities in criminal matters (2020/2016(INI)). (2022/C 132/02).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM/2021/206 final. 21 April 2021.

European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

P9_TA(2023)0236. Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial

intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

Spain

Organic Law 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

Organic Law 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

Law 36/2015, de 28 de septiembre, de Seguridad Nacional.

Organic Law 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Italy

Legge 3 dicembre 2021, n.º 205. Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.

France

Loi nº. 2023-380 du 19 mai 2023 relative aux Jeux Olimpiques y Paralympiques de 2024.

RECCOMENDATIONS AND OTHER TEXTS

United Nations Development Programme, *Human Development Report*, 1994.

Committee on the Rights of the Child, *General Comment Nº. 10 (2007) children's rights in juvenile justice*, Geneva, 2007.

OECD, *Recommendation of the Council on Artificial Intelligence*. C/MIN(2024)16/FINAL.

UNESCO, *Recommendation on the Ethics of Artificial Intelligence,* adopted in Paris on 23 November 2021.

Opinion 4/2007 on the concept of personal data adopte don 20th June by Group of Work Data Protection Working Party.

EUROPEAN COMMISSIOIN FOR DEMOCRACY THROUGHT LAW (Venice Commission) & OSCE OFFICE FOR DEMOCRATIC INSTITUTIONS AND HUMAN RIGHTS (OSCE/ODIHR), *Guidelines of Peaceful Assembly (3rd Edition)*, 2019.

Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024 (demande d'avis n° 22017438).

Council of Human Rights, *The right to privacy in the digital age*, 2021.

COUNCIL OF EUROPE. *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*, 2019.

HUMAN RIGHTS COUNCIL: *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai*, 2012. A/HCR/20/27.

- *Report of the Special Rapporteur on the rights to freedom of peaceful assambley and association*, 2019.

UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *Impact of new technologies on the promotion and protection of human rights in the contexts of assemblies, including peaceful protests*, 2020. A/HRC/44/24.

HIG-LEVEL EXPERT GROUP ON AI, *Ethics Guidelines for Trustworthy Artificial Intelligence*, 8 April 2019.

VENICE COMMISSION: *Opinion on video surveillance in public places by public authorities and the protection of human rights.* Study nº. 404/2006, Adopted at its 70th Plenary Session (Venice, 16-17 March 2007). CDL-AD(2007)014.

- *Report on the Democratic Oversight of the Security Services*. Study nº. 388/2006, Adopted at the 71st Plenary Session (Venice, 1-2 June 2007). Strasbourg, 11 June 2007. CDL-AD(2007)016.

AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE. *Possible elements of a legal framework on Artificial Intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law*, Strasbourg, 3 December 2021. CAHAI(2021)09rev.

Comité Consultatif d'Éthique pour les Sciences de la Vie et de la Santé, *Biométrie, données identifiantes et droits de l'homme*, Avis nº. 98, 2007.

JURISPRUDENTIAL APPENDIX

Court of Justice of the European Union

CJUE (Grand Chamber) of 9 November 2010, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. ECLI:EU:C:2010:662.

Opinion of Advocate General Mengozzi of 13 June 2013, Case C-291/12. Michael Schwarz v. Stadt Bochum. EU:C.2013:401.

CJEU (Grand Chamber) Joined Cases C-293/12 and C-594/12, 8 April 2014. *Digital Rights Ireland Ltd.* ECLI:EU:C:2014:238.

CJUE (Grand Chamber), Case C-131/12 de 13 de mayo de 2014, *Google Spain v. Agencia Española de Protección de Datos*. ECLI:EU:C:2014:317.

CJUE (Gran Chamber) Joined Cases C-203/15 and C-698/15, 21 December 2016. ECLI:EU:C:2016:970.

CJEU (Grand Chamber) Case C-207/16, 2 October 2018. ECLI:EU:C:2018:788.

CJEU (Grand Chamber) Joined Cases C-511, 512 y 520/18, 6 October 2020, *La Quadrature du net and others*. ECLI :EU:C:2020 :791.

CJEU (Grand Chamber) Case C- 520/18, 6 October 2020, *Ordre des barreaux francophones et germanophones*. ECLI:EU:C:2020:7.

CJEU (Grand Chamber, Case C-311/18, 16 October 2020, *Facebook Ireland and Schrems.* ECLI:EU:C:2020:559.

European Court of Human Rights

ECHR *Case Klass and others v. Germany*, 6 September 1978, nº. 5029/71.

ECHR *Case Malone v. The United Kingdom*, 26 April 1985, nº. 8691/79.

ECHR *Case Leander v. Sweden*, 26 March 1987, nº. 9248/81.

ECHR *Case Murray v. The United Kingdom*, 28 October 1994, nº. 14310/88.

ECHR *Case Friedl v. Austria*, 31 January 1995, nº. 15225/89.

ECHR, Case *C.R. v. The United Kingdom*, 22 November 1995, nº. 20190/92.

ECHR *Case Osman v. The United Kingdom*, 28 October 1998, nº. 87/1997/871/1083.

ECHR *Case Amann v. Switzerland*, February 16 2000, nº. 27798/95.

ECHR *Case P.G and J.H.. v. The United Kingdom*, 25 September 2001, nº. 44787/98

ECHR *Case Peck v. The United Kingdom,* 28 January 2003, nº. 44647/98.

ECHR, *Case Djavit An v. Turkey*, 20 February 2003, nº. 20652/92.

ECHR *Case S. and Marper v. The United Kingdom*, 4 December 2008, nº. 30562/04 and 30566/04.

ECHR *Case Reklos and Davourlis v. Greece*, 15 April 2009, nº. 1234/05.

ECHR *Case Gardel v. France*, 17 March 2010, nº. 16428/05.

ECHR *Case Uzun v. Germany*, 2 December 2010, nº. 35623/05.

ECHR *Case of Association "21 December 1989" and others v. Romania*, May 24 2011, nº. 33810/07.

ECHR *Case SH and others v. Austria*, 3 November 2011, nº. 57813/00.

ECHR *Case Shimolovos v. Russia*, 28 November 2011, nº. 30194/09.

ECHR *Case Von Hannover c. Germany (nº. 2)*, February 7 2012, nº. 40660/08 & 60641/08.

ECHR *Case Piechowicz v. Poland*, 17 July 2012, nº. 20071/07.

ECHR *Case Peta Deutschland v. Germany*, 8 November 2012, nº. 43481/09.

ECHR *Case Dervishi v. Croatia*, 25 December 2012, nº. 67341/10.

ECHR *Case Szabó and Vissy v. Hungary*, 12 January 2016, nº. 37138/14.

ECHR *Case Vukota-Bojić v. Switzerland*, 18 January 2017, nº. 61838/10.

ECHR *Case Ben Faiza v. France*, 8 May 2018, nº. 31446/12.

ECHR *Case S.J.P and E.S. v. Sweden*, 28 November 2018, nº. 8610/11.

ECHR *Case Catt v. United Kingdom* January 24 2019, nº. 43514/15.

ECHR *Case Altay v. Turkey*, April 9 2019, nº. 11236/09.

ECHR *Case Catt v. The United Kingdom*, 24 April 2019, nº. 43514/15.

ECHR *Case López Ribalda and others v. Spain*, October 17 2019, nº. 1874/123 & 8567/13.

ECHR *Case Papageorgiou and others v. Greece*, 31 October 2019, nº. 4762/18 and 6140/18.

ECHR Case *Frâncu c. Roumanie*, 13 January 2020, nº. 69356/13.

ECHR *Case of P.N. v. Germany*, 11 June 2020, nº. 74440/17.

ECHR *Case Gaughran v. The United Kingdom*, June 13 2020, nº. 45245/15.

ECHR *Case Breyer v. Germany*, 30 January 2020, nº. 50001/12.

ECHR *Case Big Brother Watch and others v. The United Kingdom*, 25 May 2021, nº. 58170/13, 62322/14 and 24960/15.

ECHR *Case of Centrum För Rättvisa v. Sweden*, 25 May 2021, nº. 35252/08.

ECHR *Case Yefimov and youth human rights group v. Russia*, 7 March 2022, nº. 12385/15 and 51619/15.

ECHR *Case Gluhim v. Russia*, 4 July 2023, nº. 11519/20.

ECHR *Case Internationale Humanitäre Hilfsorganisation e.V. v. Germany*, 19 February 2024, nº. 11214/19.

Spain

SCC 33/1982, 8 June 1982, [1982/33].

SCC 59/1985, 6 May 1985, [1985/59].

SCC 81/2001, de 26 de marzo, [RTC 2001/81].

SCC, 76/2019, 22 May 2019, [RTC 2019776]. ECLI:ES:TC:2019:76.

SCC (Sala Segunda) 27/2020, de 24 de febrero, [RTC 2020/27]. ECLI:ES:TC:2020:27.

Judgment of Central Criminal Court 2/2024, 23 January 2024, [JUR 2024/49366]. ECLI:ES:AN:2024:388.

Italy

Consiglio di Stato Sezione III Sentenza 25 novembre 2021, n. 7891.

United Kingdom

High Court of Justice Queen's Bench Division. Divisional Court Sitting at Cardiff Civil Justice Center. Case R (Bridges) v CCSWP and SSHD, nº. CO/4085/2018, September 4 2019.

Germany

Jugdment of the First Chamber of the Federal Constitutional Court of Germany, of February 16, 2023 (1 BvR 1547/19, 1 BvR 2634/20).

France

Constitutional Court of France Judgment nº. 2012-652 DC, 22 March 2022.

ANNEX I
INTERVIEW WITH THE CHIEF INSPECTOR OF THE IDENTIFICATION UNIT OF THE FORENSIC POLICE IN GRENADA (SPAIN)

(Semi-structured interview model)

Good morning, I am Cristina Domingo Jaramillo, Researcher and Professor in the Department of Criminal Law at the University of Granada. I did my studies in Criminology here and I obtained my PhD in 2022 in the PhD program in Criminology. Currently, I am doing a second doctoral thesis at the University of Bologna (Italy), whose subject is precisely the use of remote biometric identification systems in the public sphere for law enforcement purposes, especially facial recognition, and how the Artificial Intelligence Act regulates them. In addition, I also analyze the benefits and possible damages that their implementation may have.

Before starting the interview, I would like to ask for your consent to record the content of what we discuss here. Your personal data will not be exposed in the text of the paper or in any subsequent publication that may result from the thesis. In addition, the information resulting from the interview will be included in the thesis as a case study to show how the ABIS system is implemented and used in our country, specifically in Granada, as an example of a facial recognition mechanism developed to prevent and control crime, as well as the impact that it has on crime.

FIRST BLOCK. Foundation and operation of the systems.

1. When did the system start to be used here in Grenada and at the national level?
2. How do these systems work, are they embedded in existing video surveillance and CCTV systems or is it rather a computer program that analyzes selected fragments of images from the time and place of interest?
3. In relation to the previous question, what type of systems are used, those that act in real time, i.e. are installed in the surveillance systems and act in a short time or delayed (with a longer time delay between recording and identification)? The IA Regulation distinguishes both typologies, establishing different requirements for each one, considering that those that intervene in real time have a greater impact on the rights and freedoms of citizens.

   (Some of the above questions will depend on the answers to questions 2 and 3). If the answer is that they are not inserted in such devices, questions 6, 7 and 13 are not asked.

4. Regarding the results of the system, does it establish a single possible identity or does it give several possibilities?
5. The role of the agents (linked to the previous one): How do they decide who is the person being searched? In case of a possible misidentification, i.e. the system has not achieved a proper match and has failed to identify the individual being searched for, how would you act?

SECOND BLOCK. Impact on crime levels. For my study it is very important to know if any impact on crime rates has been observed or is being observed because there are practically no studies on the subject. Also the effectiveness of the systems.

6. Has it been implemented in specific areas? (depends on what she answered in questions 2 and 3).
7. If so, has there been any impact on crime levels, in the sense of reducing it?
8. How many times has the mechanism been used during the time it has been in operation in Grenada?
9. Of those X number of times, how many have been successful, i.e. have led to the correct identification and subsequent arrest of the subject? Have any of them been incorrect?
10. What type of subjects have been (and are) subject to the measure and in what situations?

THIRD BLOCK. Impact on citizens' rights and freedoms.

11. What is the regulatory basis for the implementation of this system?
12. What kind of databases are used to carry out the identification, who creates or provides them, the police or private companies, what guarantees are taken into account for the respect of privacy and the protection of personal data, who is the data processor, how are the databases used to make a proper use of them?, In the sense that they guarantee a limited use of the data, that they are not excessive, adequate time frame, avoidance of data leakage, avoidance of data leakage, and the use of data that is not excessive.
13. All individuals who are passing through a public space where a facial recognition system is embedded are susceptible to be identified by the system, is it reported that such systems are being used at a given time and place in order to ensure transparency in the use of the systems?
14. How long is the image stored for?
15. When a match or identification occurs, how is the identity subsequently verified? Are other parameters used to counteract the information?

16. One of the benefits of automated facial recognition is objectivity and the elimination of racial bias on the part of the agents. In this sense, do you think it is a more objective technique than the identification carried out by the agents themselves, has a reduction of biases been observed or does the system identify certain population groups worse? (related to question 9).
17. Do you think that if the technique becomes generalized and begins to be implemented in video surveillance systems for real-time and/or delayed use, it could have an impact on citizens, in the sense that they could restrict their movements due to the fear of being identified?
18. The technique is blamed for potentially leading to a state of surveillance and monitoring of the movements of individuals. Do you believe that this situation can occur if the use of these systems is not limited?
19. Finally, how do you see the future of crime and the emerging technological measures designed to combat it?

Thank you very much for your time and collaboration. Your answers are very useful for the development of my research.

NOTA FINAL

Permítaseme realizar esta nota final en mi lengua materna. De este modo, podré expresar de forma más clara los sentimientos que me inundan a escasos días del depósito de la tesis doctoral. Además, siendo consciente de que no todos aquellos a quienes va dirigida dominan el idioma de Shakespeare, podrán entenderla sin necesidad de recurrir a ningún traductor.

El periodo que comprende desde el mes de noviembre de 2021 (momento en el que comenzaron mis estudios de doctorado en la Universidad de Bolonia) hasta la fecha de redacción de estas líneas, ha estado repleto de vivencias y personas inolvidables, a las que tengo tanto que agradecer y que, sin duda, están implícitas en cada una de las páginas que conforman la presente investigación. A todos ellos van dirigidas estas palabras de agradecimiento.

Es cierto y, no nos engañemos, la tesis se hace cuando se está estudiando y escribiendo pero, muy especialmente, cuando se comparten ideas y reflexiones con otras personas ajenas a tu ámbito de estudio. Esta es la magia del Real Colegio de España, pues permite que doctorandos provenientes de cualquier parte del territorio nacional y de cualquier disciplina confluyan en un mismo espacio, lo cual propicia el debate y el intercambio de pensamientos y opiniones (incluso las más diversas), permitiendo un enriquecimiento, no solo intelectual sino también personal.

En primer lugar, como no, al Patrono, el Ilmo. Sr. D. Iván de Arteaga y del Alcázar, y a la Junta de Patronato que él mismo preside, por haberme otorgado una de las becas "Santa Catalina de Bolonia" para realizar el *Dottorato di ricerca* en la Universidad de Bolonia, lo cual me ha brindado la oportunidad de conocer y disfrutar de esta maravillosa ciudad italiana. No solo eso sino, lo más importante, de poder vivir la experiencia del Real Colegio de España y hacerme parte de la historia de tan ilustre y distinguida institución que, a pesar de los avatares, ha permanecido en el tiempo, transmitiendo de generación en generación el legado académico y cultural de su fundador, el Cardenal D. Gil Álvarez de Albornoz.

Gracias al Magnífico Rector, D. Juan José Gutiérrez Alonso porque, con su dedicación y entrega incondicional al Colegio y sus colegiales, nos ha permitido acercarnos a la historia de este lugar, sus valores, haciendo de sus muros no solo un espacio físico donde convivir sino un auténtico hogar.

Me siento muy orgullosa de formar parte de la familia albornociana. Se me vienen tantos nombres a la cabeza, que es imposible mencionarlos a todos en este breve espacio, por lo que pido a aquellos que no se vean reflejados expresamente por escrito, me perdonen. Agradecer, por un lado, a los antiguos colegiales, quienes, aun no habiendo

compartido mucho tiempo en el Colegio, han pasado a formar parte de mi entorno más cercano; y, muy especialmente a mis compañeros coetáneos, pues sin ellos esta experiencia no habría sido tan bonita y enriquecedora. Sobre todo a aquellos que pasaron de ser compañeros a amigos y, en algunos casos, hermanos. Especialmente a Vicky, por enseñarme el verdadero valor de la amistad y encontrar en ella un apoyo incondicional. Tampoco puedo olvidarme de Aixa y Gabriel, pues ellos fueron los inductores de que comenzara esta aventura. Para ambos, mi más profundo agradecimiento.

Al Prof. Lorenzo Morillas Cueva, mi más sincera muestra de afecto y gratitud, puesto que siempre me ha apoyado –y lo sigue haciendo– en todos y cada uno de los proyectos que le propongo. Además, su pasión, entrega y dedicación a la Universidad me sirven de guía para mejorar constantemente. No he podido tener mejor Maestro.

Igualmente, quiero trasladar mi agradecimiento a mis queridos compañeros del Departamento de Derecho Penal de la Universidad de Granada, por los buenos consejos, por el gran equipo que hacemos y por estar siempre cuando les necesito.

Por último y, no por ello menos importante sino todo lo contrario, a mis amigos de siempre y a mi familia, pues son los que más han sufrido mis largas ausencias pero han entendido que forman parte del proceso. Quiero reconocer de forma particular a mis padres, por haberme transmitido sus valores, por su completa dedicación y esfuerzo diario para que haya llegado hasta aquí. Son ejemplo de lucha y sacrificio. A ellos se lo debo todo. Y, como no, a mi hermana, porque es quien siempre está a mi lado, mi compañera de vida.

En Montejícar, a 25 de enero de 2025.