UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

Università degli Studi di Modena e Reggio Emilia

DIPARTIMENTO DI STUDI LINGUISTICI E CULTURALI

Corso di Laurea Magistrale in

Languages for Communication in International Enterprises and Organizations

Safeguarding Privacy under Article 8 of the European Convention on Human Rights in the Age of Emotion Recognition Systems: A comparative Analysis of the European, American and Chinese Legal Frameworks

Prova finale di:

Elisa Valenghi

Relatore:

Vincenzo Pacillo

Correlatrice:

Basira Hussen

Anno Accademico 2025/2026

Table of Contents

Abstract

The aim of this dissertation is to analyze the impact of Artificial Intelligence, and in particular of emotion recognition systems, on the right to privacy, enshrined and protected by Article 8 of the European Convention on Human Rights (ECHR). After thoroughly examining the evolving concept of privacy in relation to the emergence of Big Data and the resulting European regulatory response aimed at regulating it, the discussion focuses on a comparative analysis of the main regulatory approaches adopted by the European Union, the United States and the People's Republic of China. The purpose of the research is twofold: on the one hand, it assesses the extent to which the use of emotion recognition systems interferes with the right to private life guaranteed by Article 8 of the ECHR. On the other hand, it aims to outline how the regulatory framework developed by the European Union differs from the approaches adopted by the United States and China, thus highlighting the main structural, regulatory and implementation differences.

Abstract

Il presente elaborato mira ad analizzare l'impatto dell'intelligenza artificiale, con particolare riferimento ai sistemi di riconoscimento delle emozioni, sul diritto alla vita privata sancito e tutelato dall'Articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU). Dopo aver esaminato approfonditamente il concetto di privacy e di vita privata in relazione all'emergere del fenomeno dei Big Data e della conseguente risposta normativa europea volta alla loro regolamentazione, la discussione verte sul confronto tra i principali modelli di regolamentazione adottati dall'Unione Europea, dagli Stati Uniti e dalla Repubblica Popolare Cinese. L'obiettivo della ricerca è duplice: da un lato si interroga in che misura l'utilizzo dei sistemi di riconoscimento delle emozioni interferisca con il diritto alla vita privata garantito dall'articolo 8 CEDU; dall'altro, si pone l'obiettivo di delineare come il quadro normativo sviluppato dall'Unione Europea differisca, sotto il profilo regolatorio e applicativo, dagli approcci adottati dagli Stati Uniti e dalla Cina, evidenziandone le principali divergenze strutturali, normative e di attuazione pratica.

Abstract

Diese Masterarbeit zielt darauf ab, die Auswirkungen der künstlichen Intelligenz und insbesondere der Emotionenerkennungssysteme auf das Recht auf Privatleben zu untersuchen, das in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) festgelegt und geschützt ist. Nach einer umfassenden Untersuchung des Begriffs der Privatsphäre im Zusammenhang mit dem Phänomen von Big Data und der entsprechenden europäischen Regulierungsmaßnahmen konzentriert sich die Analyse auf einen Vergleich der wichtigsten Regulierungsmodelle, die von der Europäischen Union, den Vereinigten Staaten und der Volksrepublik China umgesetzt werden. Das Ziel der Untersuchung ist zweigeteilt. Einerseits wird der Frage nachgegangen, welche Auswirkungen der Einsatz von Emotionenerkennungssystemen auf das durch Artikel 8 EMRK garantierte Recht auf Privatsphäre hat. Andererseits besteht das Ziel darin, die Unterschiede zwischen dem von der Europäischen Union entwickelten Rechtsrahmen und den von den Vereinigten Staaten und China verfolgten Ansätzen in Bezug auf Regulierung und Anwendung darzustellen und die wichtigsten strukturellen, normativen und praktischen Unterschiede hervorzuheben.

Introduction

The rapid and widespread development of Artificial Intelligence has radically transformed the way in which personal data is collected, processed, and interpreted in the contemporary landscape. Among the latest and most controversial advances characterizing the present technological revolution are the so-called emotion recognition systems. Having developed through the combination of affective computing and behavioral science, these systems do not merely identify an individual's biometric identity, but also seek to decode the inner psychological state, emotional responses, and inferred intentions through the automated analysis of facial expressions, subtle movements, and physiological parameters.

While these innovations undoubtedly provide opportunities of considerable commercial, medical, and public safety interest, they also raise critical ethical and legal questions. The algorithmic claim to enter the emotional sphere of human beings inevitably collides with the safeguard of fundamental human rights. Within the European context this friction is particularly relevant in relation to the right of privacy and private life enshrined in Article 8 of the European Convention on Human Rights (ECHR). Nowadays the traditional concept of privacy must evolve toward a new multifaceted dimension in order to ensure protection against automated interference, sensitive data collection, and intrusive psychological and emotional assessment.

Based on these considerations, this dissertation aims to investigate the impact of biometric surveillance technologies, with a particular focus on emotion recognition systems, by adopting a double perspective. In order to conduct a critical analysis, the present study is therefore built around two core questions: to what extent does the deployment of emotion recognition systems interfere with the right to privacy granted by Article 8 ECHR? Secondly, how does the European legal framework differ, from a regulatory and practical perspective, from the approaches adopted in the United States and China?

To address these questions, the dissertation is divided into three main chapters. The first chapter examines the legal framework governing the protection of privacy rights in the European Union, in particular Article 8 of the European Convention on Human Rights (ECHR). After tracing the evolution of the concept of privacy, private life and personal data protection, the chapter analyzes four landmark cases of the European Court of Human Rights illustrating how the notion of private life has been progressively broadened to address

the challenges arising from the development of new technologies and the phenomenon of Big Data. Finally, the chapter ends with an overview of the European regulatory framework, pointing out the shift from a traditional understanding of privacy to a more comprehensive approach to data protection, resulting in the adoption of regulatory measures such as the GDPR to ensure an effective level of privacy and data protection in the digital age.

In the second chapter the focus is narrowed to address the subject of affective computing and emotion recognition systems by analyzing their functioning, technical limitations, and related ethical implications. Following an introduction to the theoretical and technological foundations of these systems, the chapter explores the criticisms regarding their reliability, by paying particular attention to issues of context dependency and cultural variability in emotional interpretation. Despite their increasing use, such systems present significant limitations in their ability to accurately infer emotional states. Subsequently, the ethical and social risks associated with their implementation are examined, including discriminatory practices, manipulation, and invasive surveillance. In this context, the Artificial Intelligence Act is discussed as the European Union's regulatory response designed to regulate AI systems through the adoption of a risk-based approach in order to safeguard fundamental human rights.

Lastly, the third chapter provides a comparative analysis of the different regulatory approaches adopted at international level, with particular emphasis on the European Union, the United States, and the People's Republic of China. After examining the practical application of the AI Act in the European context, the chapter focuses on the U.S. model, characterized by a fragmented and market-oriented approach, and on the Chinese model, in which the regulation of AI systems is embedded in an environment strongly shaped by social order, control and national security imperatives. The comparison of these three models demonstrates how the regulation of AI and consequently of emotion recognition systems is deeply influenced by cultural, political, and legislative factors. This inevitably translates into significant implications for the protection of privacy and individual rights.

In conclusion, this dissertation aims to critically examine the relationship between technological innovation and the protection of privacy, by assessing the extent to which current regulatory frameworks are effective in addressing the challenges posed by innovative systems of data collection and automated analysis.

CHAPTER 1

1.1 Legal framework of Article 8 ECHR, the notion of Privacy and Data Protection

The European Convention on Human Rights (ECHR)[1], drafted in 1950 and following the Universal Declaration of Human Rights (UDHR) of 1948, marks the culmination of a long process of determination of human rights. In this regard, three generations of human rights law have been identified.

The first stage is defined by the so-called *liberty rights* which primarily aim to protect individuals from the power of the state. They can be understood as subjective rights requiring the state not to interfere with the legal goods such as privacy, non- discrimination, bodily integrity, freedom of movement, freedom of expression, freedom of association, freedom of religion, which are protected by such rights. Priority is thus given to the protection of individuals as autonomous actors within a democratic society, as well as to the state's negative obligations towards its citizens.[2]

Rights developed in the second generation can be defined as *social and economic rights*, as the public goods they protect concern employment, food and housing, social security, healthcare, and access to basic utilities. This second generation of human rights imposes positive obligations on states to create and sustain the goods they are required to protect.[3]

Finally, the latest part of the twentieth century witnessed the emergence of the third generation of human rights. These include rights related to the construction and development of collective identities, thus focusing on the *rights of groups.*[4]

Within this framework, the first generation of rights provides a significant conceptual foundation for Article 8(1) ECHR by stating that "everyone has the right to respect for his private and family life, his home and his correspondence"[5]. This provision outlines specific

[1] It constitutes one of the most important legal instruments for the protection of fundamental rights in Europe and aims to establish a common and coherent standard in order to safeguard human rights among its Member States. W. A. Schabas, *The European Convention on Human Rights: A Commentary*, 2015, p. 1.
[2] M. Hildebrandt, *Law for Computer Scientists and Other Folk*, 2020*,* p. 101, 102.
[3] Ibidem.
[4] Ibidem.
[5] European Court of Human Rights, *European Convention on Human Rights*, 2021, p. 11.

rights which must be guaranteed to an individual by state. The primary purpose of Article 8 is, in fact, to protect individuals against arbitrary interference with their private and family life, home and correspondence, thus representing a classic negative obligation. However, Member States also have positive obligations to ensure that Article 8 rights are respected, even in relationships between private parties. Specifically:

> "Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves." [6]

At this point, it is essential to point out that the article includes a second paragraph which stipulates that

> "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, 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."[7]

Article 8(2) clarifies that the rights protected by the letter are not absolute, as public authorities may interfere with these rights under certain circumstances. Paragraph 2 also specifies the conditions under which such interference by public authorities may be justified:

---

[6] Council of Europe, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life*, 2017, p. 8/101.
[7] European Court of Human Rights, *European Convention on Human Rights*, 2021, p. 11.

only interferences that are in accordance with the law and necessary in a democratic society to achieve one or more of the legitimate aims listed in Article 8(2) will be regarded as an acceptable limitation by the State on an individual's rights. In assessing whether the measures taken by the State are compatible with Article 8, the State is granted a certain degree of discretion, the *margin of appreciation.*[8]

The *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life* (2017) clarifies that in order to assess a State's positive and negative obligations under the Convention, one must ensure that a fair balance is maintained between the competing interests of the individual and those of the community as a whole, with the legitimate aims listed in Article 8(2) regarded as being particularly relevant. In cases involving a negative obligation, the Court must determine whether any interference is in accordance with the law, pursues a legitimate aim (which includes national security, public safety, economic well-being of the country, prevention of disorder or crime, and the protection of the rights and freedoms of others), and is necessary in a democratic society.

Furthermore, the law must be clear and accessible, thus implying that domestic law must be sufficiently foreseeable to provide individuals with an adequate indication of the circumstances and conditions under which the authorities are entitled to take measures affecting their rights under the Convention. The principle of clarity, accessibility and predictability of the law is thus emphasized since it is essential for the protection of rights.[9]

Having considered the general regulatory framework of Article 8, it is relevant for the purposes of this thesis to examine one specific aspect: the concept of *private life*. It is a broad concept that cannot be given a unique definition, and as has been exemplified, it is wider than the right to privacy, as it refers to a domain in which every individual can freely pursue the development and fulfillment of their personality. Given the wide range of aspects encompassed by private life, cases under this concept are generally grouped into three main

[8] U. Kilkelly, *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights*. Human Rights Handbooks, No. 1, 2001, p. 6.
[9] Council of Europe, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life*, 2017, p. 9/101.

categories: individual's physical, psychological, or moral integrity, their privacy, and their identity[10].

The European human rights system therefore adopts a dynamic interpretation of privacy. Such a broad understanding makes it impossible to provide an exhaustive definition of privacy, as the human rights dimension is shaped by historical, political, social, economic, and technological factors.

Having said that, however, the notion of privacy has been defined as a value, an interest, a right, or a good that can be analyzed from various perspectives: ethical, economic, political and legal. Additionally, it has been pointed out that human rights originally operated in a vertical relationship between state and its citizens, rather than in a horizontal one between private individuals.[11]

However, the economic changes resulting from the Industrial Revolution led courts to recognize the so-called *horizontal effect* of constitutional rights, such as the right to privacy. This means that the state has a duty to protect these rights, allowing citizens to hold the state responsible if it fails to prevent violations by powerful actors in the private sector. This is referred to as the indirect horizontal effect, since the rights cannot be invoked directly against private parties. The latter has been recognized by the ECtHR, mandating states to ensure effective protection against violations by non-state actors. In this sense human rights can be seen as legal tools protecting individuals against interference by both state and private actors.[12]

More specifically, privacy, in its negative dimension, protects individuals against interference in their autonomy by governments and by private actors.[13] The positive dimension of privacy has, in turn, been examined as a safeguard of core democratic values, ensuring individuals' self-determination, autonomy, and freedom of choice, as well as their right to be different. It also safeguards personal autonomy in areas such as sexuality, health, personal development, and social identity. In a nutshell it can be stated that privacy is strictly

[10] Council of Europe, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life*, 2017, p. 16/101.
[11] M. Hildebrandt, *Law for Computer Scientists and Other Folk*, 2020, p. 110, 111.
[12] M. Hildebrandt, *Law for Computer Scientists and Other Folk*, 2020, p. 111.
[13] S. Gutwirth, & P. De Hert, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power,* 2006, p. 511.

related to individuality, dignity, and autonomy, the right to it understood as the right to be left alone and to be free from external interference. It can equally be affirmed however that privacy also relates to the right to develop one's own identity, to be treated with respect, and to make independent choices regarding one's lifestyle, employment, education, and political views. In this sense, privacy falls between the right to be free from interference and the right to be free to develop one's own identity. Privacy guarantees each person's uniqueness and their ability to resist power when it is in opposition to individual interests. From this perspective, it functions as a legal safeguard against the concentration of power, thus affirming its essential role.[14]

It is particularly relevant at this point to outline the non-absolute nature of privacy by affirming that its essential role does not imply that privacy and the freedom it protects are absolute or inviolable values[15]. Indeed, it has been argued that individuals never enjoy absolute control over their privacy, as their freedom is preserved only insofar as it does not create social or interpersonal conflict. These areas of friction and conflict require careful balancing of competing rights and interests. This demonstrates that, while privacy is essential in a democratic constitutional state due to its connection with individual liberty, it is inherently a relational, contextual, and social concept, acquiring concrete significance only when it comes into conflict with other private or public interests.[16]

A further key aspect to consider for the purposes of this dissertation is the soaring expansion of digital technologies which has deeply transformed the meaning and scope of privacy. In contemporary societies, personal information is constantly generated, collected, and processed by both public institutions and private actors. Digital platforms, social networks, online services, and automated systems rely on the large-scale processing of personal data.

It is therefore unsurprising that privacy has undergone a profound transformation, gradually shifting from the traditional "right to be left alone" to what is now understood as "data protection" or "data privacy." The rapid adoption of these new information

[14] M. Hildebrandt, *Law for Computer Scientists and Other Folk*, 2020, p. 107.
[15] Ibidem
[16] S. Gutwirth, & P. De Hert, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power,* 2006, p. 528.

technologies by governments and private companies has raised concerns that secret surveillance by states or commercial entities could threaten individuals' privacy and freedoms.[17]

Additionally, the technological revolution has contributed to accelerating the shift toward a global digital society, giving rise to a wide range of transnational issues, including the circulation and use of personal data. Technology has therefore transformed personal information into an exchangeable commodity, so that privacy has become even more vulnerable. Indeed, firms and companies exploit personal data to increase profits, by profiling customers to enhance their marketing strategies.[18]

Consequently, the potential use of personal data has grown extensively, while at the same time the vast quantities and permanence of such data have intensified privacy-related risks. Personal data is often employed in ways that were not foreseen at the time of collection. Not to mention that almost every human activity leaves a digital footprint, making it easier to monitor individual behavior. Moreover, breaches of personal data security are becoming increasingly common. These increased risks highlight the necessity for more robust measures to safeguard privacy.[19]

In view of the above considerations, it is worth taking into account that the UDHR and the ECHR were drafted long before the advent of computers and the internet. While these technological developments produced noteworthy advantages, by improving productivity, efficiency, and quality of life, they have also given rise to new risks for the right to respect for private life. In response, a new dimension of privacy has emerged, often referred to as *informational privacy*, which focuses specifically on the collection, processing, and use of personal data.[20]

As will be discussed in detail later in this chapter, data protection is recognized within the EU legal framework as a fundamental right, distinct from the fundamental right to

[17] F. Petrucco, *The right to privacy and new technologies: Between evolution and decay,* 2019, p. 150.
[18] Ivi p. 150, 151.
[19] Organisation for Economic Co-operation and Development (OECD). *The OECD Privacy Framework*, 2013, p. 20.
[20] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018, p. 18,19.

respect for private life.[21] The Court of Justice of the European Union (CJEU) affirms that the two rights are distinct by adding that the right to data protection grants individuals broader rights over a wider range of data than the right to privacy. It further claims that the control over personal data provided by the right to data protection serves two purposes, as it safeguards individual personality rights that may be threatened by the processing of personal data, while helping to reduce power and information asymmetries between individuals and those who process the data.[22]

Despite this, the right to respect for private life and the right to the protection of personal data are interconnected as they both aim to safeguard similar values, such as the autonomy and human dignity of individuals. They therefore constitute a solid basis for the exercise of other fundamental freedoms, including freedom of expression, freedom of peaceful assembly and association, and freedom of religion. Even though the right to respect for private life and the right to the protection of personal data are related, as they seek to protect similar values, they differ in their formulation and scope. While, on the one hand, the right to respect for private life is based on a general prohibition of interference, on the other hand the right to the protection of personal data is regarded as a modern and active right[23], implemented through a system of checks and balances aimed at safeguarding individuals when their personal data are processed.[24]

As already pointed out in defining and differentiating the concepts of private life and privacy, data protection and privacy, although conceptually similar, can not be fully equated. Scholars have highlighted that, while privacy can be considered a tool of opacity, data protection mainly promotes transparency. More precisely, privacy is characterized by opacity, as a negative right that prevents governments and other external actors from interfering with individuals' personal sphere, while data protection can be defined as permissive in nature and transparency oriented. Since the processing of personal data is deemed lawful, data protection aims to regulate such processing in a transparent manner

[21] Data protection in Europe started in the 1970s, when several states adopted laws to control how public authorities and large companies process personal information.
[22] O. Lynskey, *Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order*. *The International and Comparative Law Quarterly*, 2014, p. 569.
[23] This aspect will be examined further in this chapter by considering and examining Article 8 of the EU Charter of Fundamental Rights together with a detailed analysis of the European regulatory framework.
[24] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018, p. 19.

through data quality principles. Only in exceptional cases does data protection adopt a prohibitive approach, for example with regard to sensitive data or processing beyond the originally specified purposes.[25]

Despite what has been stated above, it should nevertheless be noted that the debate among scholars remains open and there is no single consensus on whether privacy and data protection are completely distinct concepts. Accordingly, it has been observed that the right to data protection originates from informational self-determination, and for this reason it may not be entirely distinct from the right to privacy. In this perspective, data protection is conceptualized as the other side of the coin translated into the digital context. Since both rights function as instruments that support individual autonomy, self-determination, and human dignity, privacy and data protection should be understood as intertwined in their nature.[26]

The academic debate has also given rise to two different approaches related to data protection: the prohibitive approach and the permissive approach. While the first one considers data protection as a right that primarily prohibits the processing of personal data unless specific conditions are met, the second one deems data protection as a right that allows personal data processing through a regulation complying with principles like fairness, purpose limitation, and transparency. If on the one hand scholars following the prohibited approach argue that data protection is closely linked to the right to privacy and should be interpreted in relation to it, on the other hand supporters of the permissive approach argue that data protection is distinct from privacy and serves to empower individuals by ensuring that data is processed in a fair and transparent way.

Ultimately, although the debate over whether data protection is prohibitive or permissive is complex and often contradictory, informational self-determination [27] is considered the underlying rationale endorsed by supporters of both prohibitive and permissive approaches.[28] This concept refers to everyone's right and ability to decide what

[25] S. Gutwirth, & P. De Hert, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power,* 2006, p. 502.
[26] P. Vogiatzoglou, P. Valcke, *Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law*, 2022, p. 16.
[27] In Europe, the notion of an individual's right to informational self-determination was first articulated by the Federal Constitutional Court of Germany in 1983.
[28] P. Vogiatzoglou, P. Valcke, *Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law*, 2022, p. 19.

information about themselves is disclosed to others, and for what purposes such information may be used. More precisely, European data protection law is based on the principle that individuals should have control over personal data relating to them.[29]

1.2 Jurisprudence on privacy, data protection under Article 8 ECHR and Big Data

After having outlined the scope of Article 8 ECHR and the evolving meaning of privacy and data protection, the subsequent step is to consider how these rights are applied in practice by the European Court of Human Rights (ECtHR) through the examination of related key cases.

A first significant case to consider is *S. and Marper v. the United Kingdom* (2008)[30] as the ECtHR examined the compatibility with Article 8 of the retention of biometric data by public authorities. The case originated in two applications by two British citizens against the United Kingdom of Great Britain and Northern Ireland on 16 August 2004. The applicants complained under Articles 8 and 14 of the Convention the retention of their fingerprints, DNA samples, and DNA profile after the end of criminal proceedings against them. More precisely, the applicants complained that they had been subjected to discriminatory treatment when compared to other similar previous cases by adding that there was no reasonable or objective justification for the treatment, nor any legitimate aim or adequate proportional relationship to the aim of crime prevention.[31]

Starting from the general principle that the concept of private life is a broad term, as it encompasses multiple aspects of a person's physical and social identity, the mere storage of data relating to the private life of an individual constitutes, in itself, an interference under Article 8.[32] However, in assessing whether the personal information retained by the authorities affects private life, the Court takes into consideration the specific context in which the data have been collected and stored, the nature of the records, the way they are used and processed, and the potential outcomes derived from such use.

---

[29] F. Thouvenin, *Informational Self-Determination: A Convincing Rationale for Data Protection Law*, 2021, p. 246, 248.
[30] European Court of Human Rights, *S. and Marper v. The United Kingdom*, Applications no. 30562/04 and 30566/04, Judgment of 4 December 2008, HUDOC.
[31] ECtHR, *S. and Marper v. UK*, § 127.
[32] ECtHR, *S. and Marper v. UK*, § 66, 67.

By applying these principles to the case in question, the Court points out that all three categories of personal information retained by the authorities in this specific case (namely fingerprints, DNA profiles, and cellular samples) constitute personal data within the meaning of the Data Protection Convention[33], as they relate to identifiable individuals. Moreover, the Government also acknowledged that these three categories qualify as "personal data" under the Data Protection Act 1998[34] when held by entities capable of identifying the individuals in question.[35] The Court additionally highlights that DNA profiles and fingerprints carry sensitive personal information thus falling within the scope of private life. The Court also examined whether such interference could be justified under Article 8(2). Although the retention pursued legitimate aims, such as the prevention of crime and the protection of public safety, the Court found that the UK system failed to strike a fair balance between public interests and individual rights by stating that

> "The retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data."[36]

The Court therefore concluded that the indefinite retention of biometric data of non-convicted individuals constitutes a violation of Article 8.

This judgment turns out to be significant as it determines that large-scale storage of personal data by public authorities must always comply with the principles of

[33] "Personal data means any information relating to an identified or identifiable individual" while "data processing means any operation […] performed on personal data, such as the collection, storage, preservation, alteration […], or the carrying out of logical and/or arithmetical operations on such data". Council of Europe, *Convention 108+: Convention for the Protection of Individuals with regard to the Processing of Personal Data,* 2018, p. 7.
[34] It is "an Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information" UK Government, *Data Protection Act 1998* (c. 29), 1998.
[35] ECtHR, *S. and Marper v. UK*, § 68.
[36] ECtHR, *S. and Marper v. UK*, § 125.

proportionality, fair balance, and necessity.[37] Ultimately it is worth noting that the Court gives particular relevance to the importance of clear and detailed rules on the scope and application of personal data-storage procedures, including safeguards on data retention, storage, use, third-party access, integrity, confidentiality and destruction, in order to provide adequate protection against abuse and arbitrariness.[38]

The analysis of the *S. and Marper v. UK* case demonstrates how the collection and storage of sensitive biometric data by public authorities constitutes an interference with Article 8 if the above-mentioned principles are not respected. An additional significant case to consider is *Bărbulescu v. Romania* (2017)[39] as being the first time that the Court examined a case concerning the monitoring of an employee's electronic communication by a private employer, thus questioning the degree to which Article 8 is applicable to private actors.[40] The case originated in an application against Romania by a Romanian citizen (Mr Bogdan Mihai Bărbulescu), on 15 December 2008. Bărbulescu was dismissed in 2007 for using a company Yahoo Messenger account for personal purposes, in violation of internal regulations. The employer monitored the employee's private conversations which included intimate communications, in order to prove the misuse of the computer.

In response to the dismissal the applicant complained that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life as enshrined in Article 8 of the Convention and that the domestic courts had failed to comply with their obligation to protect that right.[41] In this regard, the Court affirms that the notion of "private life" may include professional activities as well as activities taking place in a public context. To address this case the Court questions whether the employer's restrictive rules gave the applicant a reasonable expectation of privacy. Nevertheless, an employer's instructions cannot completely erase an individual's private social life in the workplace. The right to respect for private life and the confidentiality of correspondence is still applicable, even though it may be subject to certain limitations when necessary. The Court therefore

[37] ECtHR, *S. and Marper v. UK*, § 101,102,103.
[38] ECtHR, *S. and Marper v. UK*, § 99.
[39] European Court of Human Rights, *Bărbulescu v. Romania,* Application no. 61496/08, Judgment of 5 September 2017, HUDOC.
[40] European Court of Human Rights, *Grand Chamber judgment in the case of Bărbulescu v. Romania* (application no. 61496/08), Q&A, 2017, p. 2.
[41] ECtHR, *Bărbulescu v. Romania* § 3.

states that the applicant's workplace communications fall within the scope of "private life" and "correspondence", so that principles covered by Article 8 are to be applied.[42]

By stating this the Court overturned a previous decision made in 2016[43], finding a violation of Article 8. The Court affirmed that the Romanian courts, in assessing the employer's decision to dismiss Bărbulescu, failed to strike a fair balance between the competing interests involved, namely the applicant's right to respect for his private life and correspondence, and the employer's interest in ensuring the proper functioning of the company. The Court additionally outlined how the Romanian courts failed to properly assess whether Bărbulescu had been given prior notice of the monitoring of his communications and had not examined the nature and extent of such monitoring, including the employer's access to the content of his messages.[44] Moreover, they failed to assess the specific reasons for introducing the monitoring, the availability of less intrusive alternatives, or whether the communications had been accessed without the applicant being aware of it.[45] As exemplified in the judgement, even if the distinction between the State's positive and negative obligations under the Convention cannot be precisely defined, the principles governing their assessment are alike. In both cases, particular attention must be given to determining a fair balance between the competing interests of the individual and those of the community, while considering the State's margin of appreciation.[46]

It is important to specify that the judgment does not imply that employers cannot, under any circumstances, monitor employees' communications or that they cannot dismiss employees for using the internet at work for personal purposes. However, the Court considers that States have to ensure that, should an employer take measures to monitor employees' communications, these measures are accompanied by adequate and sufficient safeguards against arbitrariness. In *Bărbulescu v. Romania* (2017) §121, the Court specifies

[42] ECtHR, *Bărbulescu v. Romania* § 71, 80, 81.
[43] The first decision was made by the Chamber of the European Court of Human Rights on 12 January 2016, stating that there had been no violation of Article 8 of the Convention. The second decision was made by the Grand Chamber of the European Court of Human Rights, which reviewed the case and concluded that there had been a violation of Article 8.
[44] The court did not assess the conduct of the private employee directly. It rather examined whether the Romanian State had complied with its positive obligations under Article 8 to protect the applicant's private life in a horizontal relationship.
[45] European Court of Human Rights, *Grand Chamber judgment in the case of Bărbulescu v. Romania* (application no. 61496/08), Q&A, 2017.
[46] ECtHR, *Bărbulescu v. Romania* § 112.

the criteria to be applied by the national authorities when assessing whether a given measure is proportionate to the aim pursued and whether the employee involved is protected against arbitrariness. One aspect is particularly emphasized: the need for the employee to be informed in advance about the possibility of monitoring, by explaining the nature, scope, and purpose of the monitoring. Without transparency, the monitoring may not meet the requirements of Article 8. Moreover, employers should not access the content of employee communications unless the employee has been clearly notified in advance. Authorities should subsequently evaluate how intrusive the monitoring is, by distinguishing between monitoring the flow of communications and accessing the actual content of messages. They should also consider whether all communications or only specific ones were monitored, the duration of the monitoring, and the number of people who had access to the collected data.[47]

Having considered the case *Bărbulescu v. Romania* (2017) as it outlines the boundaries of privacy within the context of specific professional relationships, one must bear in mind the significant development of the digital landscape throughout the subsequent years, which led to a shift from the individual monitoring to algorithmic processing of mass data and required the Court's jurisprudence to deal with increasingly complex cases.

A noteworthy example is provided by the case of *Big Brother Watch and Others v. the United Kingdom* (2021)[48] resulting in a landmark judgment by the European Court of Human Rights on mass surveillance. Unlike the previously analyzed cases, the dispute did not concern the targeted surveillance of a particular person, but rather the State's ability to intercept massive amounts of data on a global scale. The case originated in 2013 from a series of revelations made by Edward Snowden (former U.S. National Security Agency employee) who revealed the existence of large-scale surveillance programs operated by the United Kingdom's intelligence services.[49] The applicants[50] argued that their electronic communications were likely to have been either intercepted by the United Kingdom

[47] ECtHR, *Bărbulescu v. Romania* § 121.
[48] European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Judgment of 25 May 2021, HUDOC.
[49] He claimed that Government Communications Headquarters (one of the United Kingdom intelligence services) was running an operation named "TEMPORA", which allowed it to collect and store huge volumes of data. ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 15.
[50] They were a coalition of human rights organizations, privacy advocacy groups, and private individuals, among them the Big Brother Watch (UK-based NGO campaigning for privacy rights), Open Rights Group (a UK digital rights organization), English PEN (a charity promoting freedom of expression) and the Bureau of Investigative Journalism (BIJ).

intelligence services, obtained by the United Kingdom intelligence services through foreign governments' interception, and/or acquired by the United Kingdom authorities from communications service providers (CSPs).[51] Snowden additionally stated that, throughout the program TEMPORA, the Government Communications Headquarters (GCHQ) was able to access "external" communications in bulk thanks to fiber-optic cables running between the UK and North America. He added that the UK not only used this data for its own purposes, but it also gave the N.S.A. access to them (which included the content of emails, Facebook entries, website histories and the metadata).[52]

It is therefore evident that the case deals with bulk interception of cross-border communications by the intelligence services. The preliminary remarks of the Court's assessment specify how the current digital age sets new major challenges and difficulties as the majority of communications are carried out digitally and transported across global networks regardless of national borders. The Court acknowledges that surveillance that is not specifically targeted at individuals can therefore have a wide scope, extending both within and beyond the territory of the surveilling State. For this reason, safeguards are fundamental, although elusive. Unlike targeted interception, which is mainly used for criminal investigations, bulk interception is primarily employed for foreign intelligence purposes in order to detect new threats posed by both known and unknown actors. While operating, Contracting States legitimately need secrecy, meaning that little information about how such systems operate is made public, and any information, if provided, is often vague, and varies significantly across States.[53] The Court therefore recognizes that Contracting States legitimately enjoy a right to secrecy while carrying out their operations, which often results in a significant lack of public transparency.

In *Big Brother Watch v. United Kingdom* (2021) § 323, the Court furthermore acknowledges that while technology have fostered communication worldwide, both Contracting States and citizens have to face multiple threats (such as terrorism, drug and human trafficking) as several of these perils originates from international networks of hostile actors who use sophisticated technologies to communicate without being detected.

[51] ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 13.
[52] Open Society Justice Initiative. (n.d.). *Big Brother Watch v. United Kingdom*, https://www.justiceinitiative.org/litigation/big-brother-watch-v-united-kingdom, accessed 4 February 2026
[53] ECtHR, *Big Brother Watch and Others v. the United Kingdom* §322.

Such technologies also enable hostile State and non-State actors to disrupt digital infrastructures while interfering with democratic processes through cyberattacks, thus posing a severe risk to national security. As a result, when assessing bulk interception systems' compliance with the Convention, the Court must comply with safeguards against arbitrariness and abuse, given that the information about the actual operation of such systems is limited.

In light of these considerations the Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses.[54] More specifically, the Court considers that Article 8 applies at each of the four stages encompassing the bulk interception process. It observes that, while the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly serious interference, the level of interference with individuals' Article 8 right increases progressively as the bulk interception process advances. Finally, at the last stage of the process, when information about a specific individual is analyzed or the content of communications is examined by an analyst, the need for safeguards is at its highest.[55] Being classified as an interception system, bulk interception can be misused so as to affect the right of individuals to respect for their private life. Article 8, however, does not forbid its use and States enjoy a significant margin of appreciation in assessing what kind of interception system is to be adopted. Nevertheless, the margin of appreciation granted to the States have to be restricted and accompanied by a number of safeguards so as to prevent abuse and arbitrariness.[56] This leads the court to establish, in *Big Brother Watch v. United Kingdom* (2021) § 361 a more stringent set of criteria with the aim to update the six previous *Weber* safeguards by sketching eight key safeguards that domestic legal frameworks must determine to ensure that bulk interception regimes comply with Article 8 of the Convention.[57]

---

[54] The Court outlines four main stages of the bulk interception process: the interception and initial retention of communications and related communications data, the application of specific selectors, the examination of selected communications data by analysts, and lastly the retention, use, and sharing of collected data with third parties. ECtHR, *Big Brother Watch and Others v. the United Kingdom* §325.
[55] ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 330.
[56] ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 347.
[57] The safeguards include: 1. Grounds for authorization, 2. Circumstances for interception, 3. Authorization procedure, 4. Procedures of selection, examination, and use of data, 5. Precautions for sharing data to other parties, 6. Limits on duration and storage, 7. Supervision by an independent authority of compliance with the safeguards, and lastly 8. Independent ex post facto review.

Despite the existence of a theoretical legal framework, as presented above, in *Big Brother Watch v. United Kingdom* (2021) § 377 the Court highlights a deficiency in the United Kingdom's bulk interception regime under section 8(4) of RIPA[58]: namely the lack of independent authorization. The Court observed that the warrants for bulk interception were issued by the Secretary of State rather than by a judge or an independent body.[59] This means that the selection of data was not subject to prior and impartial evaluation by an independent body. Consequently, the Court concluded that the UK regime did not provide sufficient guarantees of one of the fundamental safeguards which is essential to prevent abuse and ensure compliance with Article 8 of the Convention. For these reasons just stated above, the Court "holds, unanimously, that there has been a violation of Article 8 of the Convention in respect of the section 8(4) regime".[60]

In conclusion, the *Big Brother Watch v. United Kingdom* (2021) judgment confirms that, while bulk interception can be a legitimate tool for national security, its compliance with the Convention depends on a subtle balance of powers. The Court emphasizes that as surveillance technology continues to expand extensively, becoming automated, legal safeguards must evolve accordingly in order to create a solid system for the protection of human rights. By finding a violation due to the absence of independent authorization and emphasizing the sensitive nature of metadata[61], the Court clearly states that the "legitimate need for secrecy"[62] cannot justify an opaque system lacking proper transparency. To be deemed lawful indeed a surveillance regime must operate transparently and be subject to impartial, third-party review at every stage of data processing.

The legal challenges raised by the digital processing of information are not exclusively related to the interception of communications. An additional and more intrusive

[58] The Regulation of Investigatory Powers Act 2000 is a UK Act "to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed*". Regulation of Investigatory Powers Act 2000*, 2000, p. 1.
[59] ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 377.
[60] ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 536/1.
[61] "The related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, […] they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with". ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 342.
[62] ECtHR, *Big Brother Watch and Others v. the United Kingdom* § 322.

dimension of state surveillance is displayed by the deployment of biometric data and artificial intelligence. A significant evolution in this regard is represented by the recent judgment of *Glukhin v. Russia* (2023)[63], where the Court has been called upon to assess the compatibility of facial recognition technology with Article 8 ECHR. Specifically, the case referred to above, which will be analyzed in detail below, deals with the use of live facial recognition technology[64] in public areas. The case originated on 23 August 2019 when the applicant was identified, located, and eventually arrested after having staged a peaceful solo protest in the Moscow underground carrying a life-size cardboard figure to demonstrate against the detention of another activist. As reported in the judgment "the case concerns the applicant's administrative conviction for his failure to notify the authorities of his intention to hold a solo demonstration using a "quickly (de)assembled object"". [65] During the investigation, the police used facial recognition technology to process the applicant's personal biometric data with the aim of identifying him so that he could be arrested. The Court consequently analyzes whether these actions violated the applicant's rights to freedom of expression and respect for private life enshrined in Article 8.

In *Glukhin v. Russia* (2023) § 31, the Court first defines the concept of biometric personal data as information revealing a person's physiological and biological features that can be used to identify them. It is specified that this category of data can only be processed with the individual's written consent, unless otherwise stipulated by law. Biometric data can in fact be processed without consent only in cases related to justice administration, defense, security, counterterrorism, transport security, anti-corruption, and operational-search activities. The Court subsequently clarifies that the processing of special categories of personal data (such as data revealing race, nationality, political opinions, religious or philosophical beliefs, health status, or intimate life) is generally prohibited except if the data has been made publicly available by the individual, is connected to justice administration, or is required for defense, security and for the other above listed cases.[66]

---

[63] European Court of Human Rights, *Glukhin v. Russia*, Applications no. 11519/20, Judgment of 4 July 2023, HUDOC.

[64] "Facial recognition technology (FRT) makes it possible to compare digital facial images to determine whether they are of the same person. Comparing footage obtained from video cameras (CCTV) with images in databases is referred to as 'live facial recognition technology'". European Union Agency for Fundamental Rights (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, p. 1.

[65] ECtHR, *Glukhin v. Russia* § 1.

[66] ECtHR, *Glukhin v. Russia* § 32.

It is essential to point out that the Court recognizes that the collection and storage of data about individuals by authorities constitutes an interference with their private lives, even if the data collected is solely limited to public activities. The Court has previously ruled that the actions of recording participation in anti-government demonstrations or monitoring movements in public places fall under the scope of private life as protected by Article 8. [67] The Court therefore emphasizes that even public activities, when systematically recorded and stored, could violate an individual's private life as a person's image and movements are intrinsic to identity and personal development. This interference requires justification under Article 8.

The judgment describes the actions undertaken by the police to identify and bring action against the applicant for his demonstration. The police exploited various methods[68] to collect and process his personal data, including facial recognition technology. More specifically the police used live facial recognition cameras to locate and arrest the applicant several days after the demonstration, while the collected images and video recordings were used as evidence in the proceedings against the applicant.[69]

As precisely described in *Glukhin v. Russia* (2023) § 70, the police report did not specify which search measures had been employed to identify the applicant. His attempt to challenge the lawfulness of those measures was unsuccessful, as the domestic courts dismissed his objections without providing exhaustive explanations. Considering this, it was reasonable for the applicant to believe that facial recognition technology had been used. The Government neither explicitly denied nor provided any clarification regarding the methods used for the identification. Finally, the Court detected information concerning multiple cases in Russia involving the application of facial recognition technology to identify participants in public protests, thus leading the Court to assume that this latter could actually have been used. This lack of transparency and documentation notably raised concern about potential abuse perpetrated against the applicant.

[67] ECtHR, *Glukhin v. Russia* § 67.
[68] Such as the collection and storage of photos and videos of the applicant's demonstration taken from a public Telegram channel, and the collection of video recordings from Moscow's underground surveillance cameras.
[69] ECtHR, *Glukhin v. Russia* § 68.

The Court therefore concludes that the deployment of facial recognition technology to identify and arrest the applicant, together with the storage and processing of his personal data resulted in an interference with his right to respect for private life under Article 8.[70] Indeed, any interference can only be justified under Article 8 § 2 of only if it is in accordance with the law, pursues one or more of the legitimate aims, and is necessary in a democratic society to achieve those aims.[71]

Domestic law must therefore provide appropriate safeguards to prevent any use of personal data that may generate a breach of Article 8 guarantees. The need for specific safeguards becomes even more imperative when personal data is processed automatically, particularly when the technologies involved continue to evolve into increasingly sophisticated systems. The protection guaranteed by Article 8 of the Convention would be seriously threatened by unlimited use of modern techniques that do not take into proper account the significant impact they may have on individuals' private life.[72] While collecting and processing personal data it is of paramount importance to have clear and detailed rules determining the scope and application of measures and safeguards concerning duration, storage, usage, access by third parties, procedures for preserving the integrity and confidentiality of data, as well as procedures for their destruction. These rules should accordingly provide sufficient guarantee against the risk of abuse and arbitrariness.[73]

Given this *Glukhin v. Russia* (2023) § 83 states that the Court firmly doubt that the domestic legal provisions meet the "quality of law"[74] requirement. It states that the Government did not provide any authoritative interpretation or examples of restrictive application of this provision in administrative and judicial practice. As a result, the law apparently allows the processing of biometric personal data, including facial recognition technology, without limitations on the situations, purposes, targeted categories of people, or processing of sensitive personal data. Furthermore, the Government did not mention any

[70] ECtHR, *Glukhin v. Russia* § 73.
[71] ECtHR, *Glukhin v. Russia* § 74.
[72] ECtHR, *Glukhin v. Russia* § 75.
[73] ECtHR, *Glukhin v. Russia* § 77.
[74] "[…] implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing adequate and effective safeguards and guarantees against abuse." B. van der Sloot, *The Quality of Law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases*, 2020, p. 167.

procedural safeguards for the use of facial recognition technology (such as authorization procedures and data usage and storage protocols) in Russia.

As a result, the Court determines that the processing of the applicant's personal data was not necessary in a democratic society. The applicant was in fact prosecuted for a minor administrative offense as he was not accused of any disruptive or dangerous acts, such as obstruction, property damage, or violence. In addition to this the Court considers that the employment of intrusive facial recognition technology for the purpose of identifying and arresting peaceful protesters could have a chilling effect[75] on their rights to freedom of expression and assembly.

In light of the above considerations, the Court delivers its judgment by affirming that the use of highly intrusive facial recognition technology to identify and arrest the applicant during his peaceful protest is incompatible with the principles of a democratic society. Hence, the applicant's personal data using facial recognition technology was not necessary in a democratic society thus resulting in a violation of Article 8.[76]

The cases examined in this section (namely *S. and Marper v. the United Kingdom* (2008), *Bărbulescu v. Romania* (2017), *Big Brother Watch and Others v. the United Kingdom* (2021) and *Glukhin v. Russia* (2023)) have been selected as they illustrate a clear development of the Court's approach to technological interference in relation to Article 8. Starting from *S. and Marper v. the United Kingdom* (2008) the Court established that the indefinite retention of biometric data of non-convicted individuals resulted in a disproportionate interference with the right to privacy stressing that even the mere storage of personal data directly affects private life. This principle was further developed and refined in the *Bărbulescu v. Romania* (2017) judgment, which highlighted the importance of transparency and prior notification expected by private actors in the context of workplace monitoring. The shift towards the modern digital landscape can be observed clearly in *Big Brother Watch and Others v. the United Kingdom* (2021) judgement, where the Court's

[75] "[…] may be defined as the *negative* effect any state action has on natural and/or legal persons, and which results in pre-emptively *dissuading* them from exercising their rights or fulfilling their professional obligations, for fear of being subject to formal state proceedings which could lead to sanctions or informal consequences such as threats, attacks or smear campaigns." L. Pech, *The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU*, 2021, p. 4.

[76] ECtHR, *Glukhin v. Russia* § 90.

attention shifts from individual forms of surveillance to algorithmic practices. The Court examined the compatibility of bulk interception regimes with the Convention, emphasizing the need for independent authorization processes. Ultimately, in *Glukhin v. Russia* (2023), the Court addressed the intrusive nature of artificial intelligence technologies, specifically live facial recognition systems.

It can therefore be stated that the scope of the right to privacy under the ECHR focuses on the protection of the individual. While the Convention originally aimed at imposing negative obligations on States (namely to refrain from power abuse) and on granting citizens negative rights, that is, the right not to be subjected to unjustified interference, the Court has progressively recognized the existence of positive obligations. States are therefore required to ensure the protection of privacy while acknowledging the right of individuals to develop their personality under Article 8. This implies that only natural persons may bring a case concerning the right to privacy under the Convention, provided that the claim is directly linked to their individual interests. Furthermore, the Court has stressed that an application will be declared admissible only if it relates to a concrete and direct interference with the applicant's right to privacy. Should the applicant be unable to demonstrate concrete interference with their rights, the application will be declared inadmissible by the Court. For instance, so-called *in abstracto* claims are considered inadmissible. *A priori* claims are likewise rejected, as the Court acknowledges complaints only if the injury has already materialized, while claims about future damage are in principle not taken into consideration.[77]

Additionally, it has been observed in the literature how the assessment of whether an individual's right is undermined is traditionally based on the presence or absence of interference with the right in question. Even though this approach can be considered suitable for traditional privacy issues, modern-day data processing poses a further challenge as violations originating from its use are not clearly defined in time, space and person. The difficulty for individuals in safeguarding their rights in the context of large-scale data collection has been described as twofold. In the first place, individuals are often unaware that their personal data is being collected. People are used to taking photos and videos of

[77] B. Van der Sloot, *A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle*, 2017, p. 541.

others in public spaces sharing them online without consent. Similarly, companies collect vast amounts of data through cookies and tracking tools to monitor online behaviors. Public authorities also gather a large amount of data about citizens, through multiple systems and covert surveillance by intelligence services. In most cases, individuals are not aware of these data collection practices. As a result, if people do not know that their data is being processed, they are unlikely to invoke their right to privacy. Secondly, the number of data flows in which an individual's data may be included is rocketing. It is almost impossible for a person to identify who is collecting the data, and above all whether these procedures are carried out in accordance with the legal system. In light of this, it can be stated that as living in an increasingly data-driven society, individuals cannot actually assess the legitimacy of all the data processing activities that may involve their personal information.[78]

The intensification of data collection and processing systems in the new digital era leads to what is defined as surveillance capitalism. It has been conceptualized as a modern economic system that considers private human experiences as raw material in order to create data-driven products for profit.[79] Surveillance capitalism differs from traditional capitalism by focusing on extracting behavioral surplus rather than relying on labor or goods. Behavioral surplus refers to the overload of data generated by individuals while using digital platforms. Companies realized that the surplus data could be analyzed and exploited to predict human behavior and sold to other companies. In this model, users are sources of raw material (namely human experiences) that are transported into data for the purpose of profit generation. Data is used to make predictions which forecast what individuals or groups will do in the future and are subsequently sold to businesses that use them to target ads, influence decisions, or shape behaviors. Surveillance capitalism thrives on the endless and often covert extraction of this data, bypassing user awareness and decision rights.[80]

The economic imperative underpinning this phenomenon lays the foundation for contemporary large-scale data processing. It follows that, as data extraction increases, the accuracy of predictions improves accordingly.[81]

.[78] Ivi p. 542.
[79] S. Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 2019, p. 11.
[80] Ivi p. 11,12, 21.
[81] Ivi p. 18, 19.

Nowadays, data permeates everyday life as individuals constantly generate and use it through digital devices. On the one hand, data enables the identification of specific patterns, making it possible to analyze and predict behavior for collective purposes. On the other hand, the same data can be used for surveillance and behavioral monitoring. Hence, the same data processes may lead to different outcomes depending on who carries out the monitoring and for what purposes. What may appear legitimate and socially beneficial can also be perceived as intrusive and harmful to personal integrity, depending on the intentions underlying the surveillance.[82] Within this framework lies the phenomenon of Big Data as the fundamental infrastructure in the economy of the current Digital Age.

At this point, it becomes necessary to define this phenomenon as its delineation influences the way in which Big Data is perceived, what kind of risks it can arise and above all whether legislation needs to be implemented. Various definitions of Big Data have been proposed in the literature, among which the one considered below is taken from the website of the European Data Protection Supervisor (EDPS):

> "Big Data means large amounts of different types of data produced at high speed from multiple sources, requiring new and more powerful processors and algorithms to process and to analyse. These practices and technologies could offer major benefits for economic growth and various sectors including energy transportation and health. Not all of this information is personal, but businesses and governments are more and more using big data to understand, predict and shape human behaviour. Big data is therefore a long term strategic concern for data protection and privacy regulators. It puts strain on not only privacy and data protection, but other fundamental rights including freedom of expression and non-discrimination."[83]

Despite the multiple definitions relating to Big Data, similar components can repeatedly be detected as they relate to three stages of Big Data processing, namely

[82] L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom, *Everyday life in the culture of surveillance*, 2023, p. 11.
[83] European Data Protection Supervisor. (n.d.). *Big data and the Digital Clearing House*. https://www.edps.europa.eu/data-protection/data-protection/reference-library/big-data-and-digital-clearing-house_en, accessed 9 February 2026.

collection, analysis and use.[84] In this regard its definition can be approached from several perspectives. The first one to be considered is variety, as Big Data can collect and "integrate structured and unstructured data from multiple sources into a comprehensive and readily accessible resource, whether it is text, images, voice, videos, streaming data, signals or other types of data".[85] Secondly, one has to consider the sources of data, as Big Data can gather, analyze and process data from a wide range of different sources. Lastly, one cannot fail to mention the processing for insights, as predictive analysis is crucial for Big Data. It involves the application of advanced techniques and algorithms to analyze data and uncover patterns and trends. Processing for insights is a revolutionary aspect of Big Data, as it allows organizations to uncover patterns and make predictions.[86]

A broadly recognized categorization for defining the technical and managerial aspects of Big Data is the 5Vs framework which encompasses Volume, Variety, Velocity, Value, and Verification. Velocity refers to the speed at which data is generated and transmitted; data is generated at high speed and has to be verified, processed, stored, analyzed, monitored and updated in order to create value and provide a competitive advantage. Additionally, value highlights the nature of data as being subjective and time-sensitive, depending on user needs. While raw data may have a restricted worth, its transformation and processing can generate competitive advantages. Verification subsequently ensures data accuracy and reliability as excessive and poorly organized data can lead to poor decision making. In addition to the 5Vs listed above, two additional parameters have been proposed including validity and visibility. Validity refers to the integrity of the data used to generate insights. Data validation therefore requires that relevant data remains accurate and appropriate throughout all stages of processing, so that every stage of the data lifecycle needs to be verified in order to grant reliability and correctness. Visibility, on the other hand, focuses on making data accessible for authorized users. Without visibility, it becomes impossible to effectively analyze data distributed across different platforms and systems. Making the right data visible to the right users at the right time enhances its value and usefulness, as inaccessible data is of little or no relevance.[87]

---

[84] B. Van der Sloot, and S. Van Schendel, *International and Comparative Legal Study on Big Data*, 2016, p. 17.
[85] U.G. Gupta, & A. Gupta, *Vision: A missing key dimension in the 5V Big Data framework*, 2016, p. 47.
[86] Ibidem.
[87] U.G. Gupta, & A. Gupta, *Vision: A missing key dimension in the 5V Big Data framework*, 2016, p. 48.

The above overview demonstrates how Big Data cannot be considered an isolated phenomenon, but rather as a new one which is intertwined with several concepts. The first one to be mentioned is Open Data as it involves making large datasets available for public use and analysis. Indeed, Open Data aims to enhance transparency by providing citizens more control over government actions. Open Data is closely related to Big Data, as it provides datasets that can be analyzed using Big Data systems. A further concept related to Big Data is Re-Use, which refers to the deployment of data for purposes other than those for which it was initially collected. While Open Data focuses on transparency and public access to government data, Re-Use highlights the commercial exploitation of data by businesses and private entities.[88]

An additional significant aspect for this thesis is the notion of profiling related to Big Data, as it represents one of its main applications. When large amounts of data are collected and analyzed, the results usually involve groups of people who share similar features and behaviors. These results are obtained through statistical correlations, which identify specific patterns within the data, thus allowing organizations to classify individuals into categories and to predict their actions. Several Data Protection Authorities (DPAs) have highlighted the close relationship between Big Data and profiling. Particularly, Belgian DPA has stated that existing data protection law applies to Big Data practices and that the new EU data protection framework is expected to provide at least a partial legal answer to profiling-related issues.[89]

The analysis conducted in the last part of this section has outlined the main features of Big Data, stretching from its economic relevance to its technical dimensions. Having defined this phenomenon, it is particularly significant at this point to examine the European regulatory framework, as Big Data may potentially interfere with the rights of individuals. The next section will indeed explore how the European Union seeks to provide a comprehensive legal response to the challenges generated by Big Data use, in order to enforce safeguards in the current digital age.

[88] B. Van der Sloot, and S. Van Schendel, *International and Comparative Legal Study on Big Data*, 2016, p. 17,18.
[89] Ivi p. 19.

1.3 Regulatory framework in Europe

In order to properly outline the European regulatory framework with regard to data protection, it is first necessary to briefly summarize its evolution over the decades. As discussed in academic discourse, the first generations of data protection stemmed in the late 50's from the computer revolution. They were mainly characterized by a national approach, meaning that regulations were implemented at different times and the protection and remedies provided varied extensively. The notion of data protection in this period was strictly related to the idea of control over information accompanied by a rising concern of citizens about social control; hence, the first generation of regulations represented the solution adopted by legislators to address the increase in social concern. It aimed to enhance transparency in data processing by ensuring citizens' right to access information, rather than to spread and democratize control over data. They provided individuals with the ability to identify who held their data, what information was collected, and the purposes for its use, yet with no room left for individual consent. Information indeed was primarily collected by public entities for public interests, turning it into a mandatory process that left no room for individuals to negotiate the use of their personal data. A further factor that prevented self-determination was the limited understanding and the significant challenge for the average person to grasp how computers worked and operated.[90]

The period from the mid-1970s to the 1990s is subsequently considered as marking the era of distributed computing, during which personal computers became widely available at affordable prices. In this phase, direct marketing underwent a significant shift towards new computerized strategies. These relied on customer profiling, which involved extensive data collection and the employment of increasingly sophisticated software. The primary goal of profiling was to tailor personalized commercial offers to individual consumers. Thus, information collection focused on selling specific products to targeted individuals. Consequently, the data subject gained a central role, as personal information acquired an economic and business value due to its pivotal role in driving sales.[91]

[90] A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics*, 2014.
[91] A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics*, 2014.

The landmark of this second generation is represented by Directive 95/46/EC also known as the Data Protection Directive[92] adopted on October 24, 1995 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data". [93] The Directive recognized personal information as a fundamental right, emphasizing the importance of protecting individuals' data as stated by Article 1(1): "[…] Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".[94] However, the primary objective of these regulations was to facilitate economic interests by ensuring the free flow of personal data across borders within the European Union as claimed by Article 1(2): "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1".[95] The European approach to data protection has been described as being grounded in the concept of personal rights, which stresses the protection of individual autonomy and dignity. [96] This makes the European framework less focused on market-driven considerations compared to other legal systems. As a matter of fact, Article 14 states that

> "Member States shall grant the data subject the right: (b) to object, […] to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."[97]

[92] The Directive was repealed and replaced by the General Data Protection Regulation (GDPR) in May 2018.
[93] European Union, *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,* 1995.
[94] Ibidem.
[95] Ibidem.
[96] A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics*, 2014.
[97] Ibidem.

Directive 95/46/EC highlighted this aspect in Article 17 by emphasizing the role of public authorities in safeguarding individuals from the involuntary or unfair exploitation of their personal data:

> "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[98]

In this new data-driven economy, personal data cannot be exploited for business purposes without the involvement of the person concerned. It is essential for data subjects to be involved in the negotiation process, as personal data is primarily used by private companies for profit, rather than solely by government agencies for public interests. As a result, the "notice and consent" model was introduced as an additional layer to the existing framework, in order to emphasize transparency and user access to information, as self-determination in data processing requires clear and prior notification.[99] However, one aspect that cannot be overlooked is that in the 1980s and 1990s, even though data analysis improved in quality, its level of complexity was relatively limited. As a result, consumers could grasp the connection between data collection and its intended uses. During this period, informed consent was regarded as a synonym of self-determination.[100]

The transition towards the third generation of data protection is driven by the advent of Big Data. The modern digital landscape has been characterized by a growing centralization of information, controlled by a limited number of public and private actors (referred to as "data barons"). The bulk of information collected constitutes a strategic and economic resource allowing them to exercise control over the information derived from their databases. In the context of Big Data however, the possibility to access data is not

[98] Ibidem.
[99] As specified in Article 7 and Article 8 of the Directive 95/46/EC.
[100] A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics*, 2014.

enough. Effective management requires professionals and advanced computing resources to analyze and interpret the data. Control over information extends beyond restricted data to include open data, as information intermediaries generate an added value by using specialized tools and analytics to process and gain insights from it. The power of data barons is not limited to expensive hardware and software, nor to the employment of skilled professionals capable of interpreting data analytics results. The core of their power lies actually in the extensive databases they possess. These data silos are not freely accessible as they are either directly generated or indirectly accumulated as part of the operations data owners. A further important aspect to consider is that modern data collection focuses less on individual profiling and more on analyzing large-scale patterns, behaviors, and attitudes of groups, and even entire nations, thus fueling concern about widespread social surveillance.[101]

The traditional data protection framework of the 1990s has been described as entering a period of crisis, as new technologic and economic developments have undermined its core principles: the purpose specification principle, the use limitation principle, and lastly the "notice and consent" model. The emergence of Big Data analytics actually “make it difficult to provide detailed information about the purposes of data processing and the expected outputs. Since Big Data analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, the description of these purposes is becoming more and more “evanescent”.[102]

One of the main challenges when it comes to Big Data is precisely linked to the fact that Big Data processes often do not pursue precise aims, so that vast amounts of data are simply collected independently from their value or potential use. Moreover, Big Data analysis merges several kinds of databases with different types of data, so that original purpose for which the data was collected gets lost.[103] Additional risks associated with the phenomenon of Big Data include privacy endangerment through re-identification of anonymized data, inaccurate data quality, and lack of transparency in data processing. Considering the multifaceted and complex nature of Big Data and the risks it entails, it has

[101] Ibidem.
[102] Ibidem.
[103] B. Van der Sloot, and S. Van Schendel, *International and Comparative Legal Study on Big Data*, 2016, p. 29.

been suggested that new norms and guidelines should be drafted and applied alongside the current regulatory framework. It is of utmost importance that already existing data protection principles such as lawfulness, fairness, proportionality, data subject rights, and purpose limitation, must not be endangered by the rise of Big Data. Moreover, individuals' rights to informational self-determination should act like a cornerstone in modern information society and, as such, it should be accordingly safeguarded by a solid data protection framework that ensures effective protection for individuals while balancing lawful and legitimate interests.[104]

Despite this, it is evident that the regulation of Big Data poses significant challenges. At first, the detection of an appropriate starting point for its definition is a complex task. While current regulations revolve around individual interests and their rights as human beings (such as privacy and personal data protection), Big Data entails the processing of aggregated data, general patterns and group profiles. As a result, whether the focus on the individual and personal data can still be deemed reasonable in the Big Data age is under question. Secondly, determining a specific entity who can act as the data controller and ensure compliance with regulatory principles in Big Data processes is equally challenging. Eventually, one must consider the significant transformation of the nature of data, which became increasingly dynamic, undergoing constant changes throughout its lifecycle. More precisely, data follows a circular path: it is at first aggregated, and anonymized. Subsequently it is de-anonymized, enriched with additional data and profiles, thus generating identifiable information and potentially sensitive data. Eventually, it can be further exploited for statistical analysis or for the creation of group profiles. Despite this, the traditional legal framework is designed around relatively static stages of data, by regulating them independently.[105]

Starting from the general considerations outlined above, one should consider that a pivotal stage in the European legal evolution is represented by the proclamation of the Charter of Fundamental Rights of the European Union (CFREU) which was proclaimed in 2000 and became legally binding with the Treaty of Lisbon in December 2009. The key difference between the EU Charter of Fundamental Rights and previously drafted human

[104] Ibidem.
[105] Ivi p. 38,39,40.

rights documents[106] is the recognition of the right to data protection as an independent right and not as a subordinate category of the right to privacy. While Article 7 of the Charter enshrines the respect for private and family life, Article 8 defines the protection of personal data by declaring that

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. 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.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."[107]

As has been highlighted in legal scholarship, data protection rules are more effective than privacy rights in preventing harms such as discrimination. By restricting decisions solely based on automated data processing, data protection laws reduce the deployment of biased proxies or assumptions that could negatively impact individuals. Data protection thus restricts decision-makers from making decisions based on automated data processing. These laws require human intervention to ensure fairness and reduce the risk of errors, biases, or discrimination.[108]

It is relevant to point out that while almost all data retention instruments generate an interference with the right to data protection, not all of them generate an illegal infringement. As reported by Article 52(1) of the EU Charter

---

[106] Such as the European Data Protection Directive
[107] European Union, *Charter of Fundamental Rights of the European Union (2000/C 364/01),* 18 December 2000.
[108] O. Lynskey, *Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order*, 2014, p. 588.

> "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[109]

In this regard the Court of Justice of the European Union (CJEU) states that any activity involving the processing of personal data constitutes an interference with the fundamental right to personal data protection under Article 8 of the EU Charter. This means that as soon as personal data is processed, the activity falls within the scope of Article 8. The Court affirms that activities such as the retention, access, or use of personal data, irrespective of the nature of the information concerned, fall within the scope of Article 8 and must consequently comply with its requirements.[110] After having established an interference, in order to determine if it is in accordance with the law, the four criteria of Article 52(1) need to be applied: essence, legitimate objective, legality, and proportionality.

The legal framework implemented by the EU Charter is further reinforced by the Convention for the protection of individuals with regard to the processing of personal data, namely Convention 108+. It is a modernized version of the original 1981 Council of Europe Convention and retains international status as it represents the first legally binding international instrument in the data protection field.[111] As specified in Article 1

> "The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy."[112]

---

[109] European Union, *Charter of Fundamental Rights of the European Union (2000/C 364/01),* 2000.
[110] P. Vogiatzoglou,, & P.D. Valcke, *Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law*, 2022, p. 33,34.
[111] Council of Europe (n.d.), *Convention 108 and Protocol*, https://www.coe.int/en/web/data-protection/convention108-and-protocol accessed 9 February 2026.
[112] Council of Europe, *Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+)*, 2018, p. 7.

It can be stated that 2018 marked a turning point concerning data protection regulation. While, as mentioned above, Convention 108+ was adopted on an international scale, in May 2018 the General Data Protection Regulation (GDPR) became fully applicable in the European Union. It is considered an extension and refinement of existing requirements imposed by the 1995 Data Protection Directive.[113] More precisely, GDPR pushes companies to manage personal data in a more responsible way, by carefully planning its collection, use, and destruction. It additionally elevates privacy to the level of other laws, such as antitrust and foreign corrupt practices law, by introducing fines and enforcement mechanisms to ensure compliance. Companies are required to impose contractual limits on data usage, extending protection even to third parties. Even more relevant is the fact that GDPR specifies that consent must be of high quality and considered equal to important life decisions.[114] It also highlights that consent must be freely given in order to be considered valid.[115] GDPR also fosters systems that involve human monitoring in decision-making processes, emphasizing the importance of data accuracy and individuals' rights to correction. The Regulation also promotes a model based on direct, first-party relationships between individuals and companies by imposing more stringent conditions on third-party data processing in order to promote transparency and direct data relationships.[116]

After having outlined GDPR general implications it is necessary to determine when it applies, namely when personal data[117] are processed. According to Article 4(2) of the Regulation

---

[113] C.J. *Hoofnagle*, B. van der Sloot, & F. Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*. *Information & Communications Technology Law*, 2019, p. 65.

[114] Article 7(4) GDPR states that: "When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

[115] C.J. Hoofnagle, B. van der Sloot, & F. Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*. *Information & Communications Technology Law*, 2019, p. 79.

[116] Ivi p. 68, 69.

[117] "personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". European Union, *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*

"'processing' means any operation […] which is performed on personal data [...], whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[118]

This definition determines that personal data processes occur every time that an organization gets in touch with data related to an individual regardless of the nature of the data collected (may it be public or private, sensitive or non-sensitive, directly or indirectly identifying a person).[119] A further aspect to be considered is the cross-border application of GDPR. The regulation not only applies to companies within the EU borders, but also to those outside the EU if they consciously process personal data of individuals who reside in the EU. Additionally, both governmental organizations and private organizations which process personal data on a large scale or that process sensitive personal data are required to appoint a representative[120] within the EU.

GDPR further specifies the legal justifications for data processing, which are based on six main grounds. In this regard, these have been comprehensively summarized in the literature. The first is the consent of the data subject, followed by contractual necessity, whereby data processing is required for the performance of a contract with the data subject. The third point is characterized by legal obligation, meaning that data processing is required in order to comply with such an obligation. Subsequently vital interest is identified as one

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, Article 4(1).

[118] European Union, *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)*, 2016

[119] C.J. Hoofnagle, B. van der Sloot, & F. Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*. *Information & Communications Technology Law*, 2019, p. 72.

[120] "'representative' means a natural or legal person established in the Union who, designated by the controller or processor […], represents the controller or processor with regard to their respective obligations under this Regulation". European Union, *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)*, 2016, Article 4(17).

main ground, meaning that data processing is necessary to protect the life of a data subject. Another permitted case for data processing is when it happens in order to accomplish a public task. Finally, the last criterion is legitimate aim, meaning that the interests of the data collector prevail over the interests of the data subject.[121]

In order to provide a comprehensive overview of GDPR it is relevant to determine the exception to its application. The regulation in fact does not apply to data processing for personal or household activities. It additionally does not encompass data processing for national security purposes or the prevention and prosecution of criminal offenses. In addition to this the Regulation recognizes that data protection may interfere with other fundamental rights; for this reason, Member States are responsible for balancing these rights, by assessing whether a limitation is necessary in order to safeguard other fundamental rights or public interests.[122]

An additional key point that is relevant to the purpose of this thesis is the notion of sensitive data under GDPR. Article 9(1) clearly states that

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."[123]

Cases in which the above-mentioned provision does not apply are expressed in Article 9(2). The GDPR actually allows processing of special categories of data when data are manifestly made public by the data subject, or when the data subject has given explicit consent to their processing.[124] Additionally, it has been observed that Europeans enjoy

[121] C.J. Hoofnagle, B. van der Sloot, & F. Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*. *Information & Communications Technology Law*, 2019, p. 76.
[122] Ibidem.
[123] European Union, *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)*, 2016.
[124] GDPR Article 9(2) (a), (e).

extensive data subject rights, including the ability to access, correct, and delete their personal data, as well as the right to object to or limit its processing. While these rights have been already determined in the earlier Directive, the GDPR provides a more detailed definition. More specifically, it outlines seven key rights for individuals: the right to access their data, transfer it to another platform (data portability), correct inaccuracies, restrict processing, object to certain uses, request data deletion, and object to automated profiling. If on the one hand the Charter of Fundamental Rights of the European Union grants right of access to their personal data, on the other hand, under GDPR, data subjects have the right to know if their personal data is being processed. If so, they are entitled to receive details about the purposes of processing, the types of data being processed, how long the data will be stored, and who the recipients of the data are.[125]

In relation to profiling and automated decision-making, GDPR introduces a specific rule that can be found in Article 22 (1) declaring that: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[126] This article clearly states that fully automated decision-making is generally prohibited. Data controllers are allowed to do it only in three cases: 1) when the decision is necessary to execute a contract between the data subject and the controller, 2) when the decision is permitted under EU or national law, or 3) when the decision is based on the explicit consent of the data subject.[127] Hence, GDPR aims to bridge the gap between established legal principles from the Data Protection Directive and their practical implementation. In order to achieve its aim, it introduced additional obligations for data controllers and further clarified the rights of data subjects.[128]

[125] C.J. Hoofnagle, B. van der Sloot, & F. Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*. *Information & Communications Technology Law*, 2019, p. 80.
[126] European Union, *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)*, 2016.
[127] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law,* 2018, p. 359.
[128] C.J. Hoofnagle, B. van der Sloot, & F. Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*. *Information & Communications Technology Law*, 2019, p. 92.

In conclusion, this analysis demonstrates that the GDPR acts as a regulatory instrument specifically designed to recalibrate power in the digital age. The Regulation addresses the structural imbalance between large organizations and individuals, by intensifying not only the role played by consent, but also by placing an increased responsibility on data controllers through the principle of accountability. Ultimately, the GDPR enforces the fundamental values enshrined in the EU Charter into concrete legal obligations. In a Big-Data-shaped society it aims to ensure the transparency of the processing of personal information so that it complies with human dignity and rights, rather than being driven merely by technological efficiency or commercial interests.[129]

Alongside the GDPR, which regulates the processing of personal data, the European Union has recently taken a further step forward by adopting the EU Data Act, effective from September 2025, to specifically address the challenges posed by the generation, access and reuse of data in the digital market. In 2020 the European Commission highlights how data-driven technologies have transformed both the economic and social landscape. It additionally recognizes that innovations produced by data offer significant benefits for citizens. However, it is crucial to ensure that data collection and usage align with European principles, fundamental rights, and regulations in order to gain the trust of citizens. The EU thus aims to become "a leading role model for a society empowered by data to make better decisions – in business and the public sector".[130] To achieve this goal the EU requires a solid legal framework which encompasses data protection, fundamental rights, safety and cyber-security. Moreover, The European Commission has to face several challenges as a few major Big Tech companies control a significant portion of global data, which may hinder the growth, innovation, and emergence of data-driven businesses within the EU. Even though it has the potential to gain success in a data-driven economy, competitors like the U.S. and China are advancing at a fast pace adopting differing approaches to data access and use.[131] In order to be successful, the EU has to adopt a balanced approach that promotes data flow and usage while maintaining high standards of privacy, security, and ethics. Since 2014 the Commission has introduced several measures, with the General Data Protection Regulation (GDPR) as the main example, which established a solid framework for digital trust in the

[129] Ibidem.
[130] European Commission, *A European strategy for data*, Brussels, 2020, p. 1.
[131] As will be discussed later in chapter 3 of this thesis.

EU. Nevertheless, the increasingly rapid technological innovation and the widespread use of Big Data make it clear that the measures adopted so far are not sufficient to respond to the complexity of the phenomenon.[132]

As a starting point, the "Bureau Européen des Unions de Consommateurs (BEUC)" highlights that, while aiming at creating a single market for data, the distinction between personal data and non-personal data is of paramount importance. While non-personal data can be commercialized through contracts, personal data is considered a fundamental right protected by the General Data Protection Regulation (GDPR) and cannot be treated as a tradable good. BEUC also establishes that the importance of a consumer-centric approach to data governance is crucial to ensure competition, consumer choice, and innovation that is beneficial to society. Safeguarding consumers' opportunity to exercise control over their data is a key element in order to foster a healthy and competitive digital ecosystem.[133]

Data control and protection face an even greater challenge due to the implementation of IoT[134] devices and digital services through which consumers provide and give birth to a massive amount of personal information. Consumers consequently struggle to manage the flow of their personal information and are uncertain with whom companies share their data and for what purposes. Even when privacy policies are provided, they are deliberately vague and frequently written in a complex and unclear language. Given this, BEUC endorsed the European Commission's initiative to introduce measures within the Data Strategy aimed at strengthening individuals' ability to enforce their data protection and privacy rights. It is additionally stressed that new measures have to be combined with a consistent enforcement of the already existing GDPR. Precisely stated, data protection authorities must grant that companies fully comply with GDPR provisions. This includes verifying whether businesses possess a valid legal basis for processing personal data which sticks to GDPR principles.[135]

---

[132] European Commission, *A European strategy for data*, Brussels, 2020, p. 2, 3.
[133] BEUC, *A European Strategy for Data: BEUC's response to public consultation*, 2020, p. 1,2.
[134] As explained in the *Handbook on European data protection law* "The Internet of Things (IoT) represents the next step in the development of the internet: the Web 3.0 era. With the IoT, devices may be connected and interact with other devices through the internet. This enables objects and people to be interconnected through communication networks, to report about their status and/or about the status of the surrounding environment". European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law,* 2018, p. 362.
[135] BEUC, *A European Strategy for Data: BEUC's response to public consultation*, 2020, p 4.

The Data Act fits within this framework, which is characterized by an increasingly complex and multilayered scenario. Its main purpose is to grant IoT users improved access to the data generated by IoT devices, which are often under the control of device manufacturers. In order to do this, the Data Act introduces new rights for users, mainly to access and share data generated by their IoT devices. This new set of rights is intended not only to empower users, by enabling them to enjoy additional services, but also to facilitate the use of IoT data by innovating firms.[136]

The Data Act particularly aims to achieve five objectives. The first one is to facilitate users to access and share the data generated through IoT devices[137], followed by the intention to allow public sector bodies and EU institutions to use data held by enterprises in exceptional situations. A further key objective is to facilitate exchanges between data processing services, such as cloud and edge providers. This ensures that users are no longer bound to a single provider and can move their digital assets freely, so that a more competitive market can be assured. Another step undertaken by the Data Act is a safeguard to prevent unlawful and unauthorized data transfer without proper notification. Lastly, it aims to set interoperability standards in order to facilitate the reuse of data across different economic sectors. In this sense the Data Act aims to create an interconnected European data market where information can flow without barriers. It can be summarized that in addition to its primary goal of empowering users to access and control their data, the Data Act also aims to safeguard and enhance competition, drive innovation, and ensure fairness within the digital economy.[138]

In order to conclude the examination carried out in the course of this section, it can be stated that Data Act does not replace its forerunner, the GDPR, but rather it aims to complete

[136] W. Kerber, *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, 2022, p. 2.
[137] Article 3 sets the obligation to make product data and related service data accessible to the user. Article 3(1) states that: "Connected products shall be designed and manufactured […] in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user." Article 5 relates to the right of the user to share data with third parties and the duty of the data holder to make the data available. Article 5(1) exemplifies: "Upon request by a user, […] the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format [...].
[138] G. Colangelo, *European Proposal for a Data Act: A First Assessment*, 2022, p. 8, 10.

it by shifting the focus from the protection of data to the actual use of this latter and its economic asset. While the GDPR focuses on the individual as a subject to be protected from privacy violation, the Data Act considers users as active agents who should be able to legitimately make use and dispose of the data they generate. Ultimately it can be stated that the Data Act and the GDPR are two sides of the same coin. While GDPR ensures data protection, the Data Act establishes that this latter can be used to foster innovation and develop competition within the European Union.

CHAPTER 2

2.1 Affective computing and emotion recognition systems

While in the first chapter the concepts of privacy and the fundamental right to private life have been defined and examined, it has also been explored how these notions have evolved over time. Particularly, it emerged how the constant development of innovative technologies, coupled by the evolution of Big Data, made it necessary to enhance and foster an adequate European regulatory framework. The latter is essential to guarantee and preserve the fundamental rights enshrined in the ECHR within an increasingly digitized society. The phenomenon of Big Data and deep learning[139] paved the way to a new frontier of data extraction, shifting the focus from behavioral patterns to subjective emotional states, thus fueling the development of emotion recognition systems and more specifically of facial emotion recognition.

Generally speaking, emotion recognition can be defined as the ability to understand one's emotional state by observing both physical and biological signals, such as facial expressions, tone of voice, gestures, as well as involuntary changes in heart rate and breathing. In a nutshell, emotion recognition is referred to as the ability to decode human emotions based on an individual's physiological and behavioral responses. Within this framework facial emotion recognition can be deemed as a subset of emotion recognition systems. Indeed, it refers to specific technology which analyses facial expressions from static images or video with the aim of gaining information on one's emotional state. Facial emotion recognition processes entail three major steps, which include face detection followed by facial expression detection and lastly the pairing of the detected expression to a specific emotional state.[140]

The aspiration to detect and categorize human emotions by analyzing physiological and behavioral signals by means of technological devices finds its theoretical and scientific

[139] Deep learning technology "is considered as one of the hot topics within the area of machine learning, artificial intelligence as well as data science and analytics, due to its learning capabilities from the given data. [...] DL is considered as a subset of ML and AI, and thus DL can be seen as an AI function that mimics the human brain's processing of data." I. H. Sarker, *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, 2021, p. 1.
[140] European Data Protection Supervisor (EDPS), *TechDispatch 1/2021: Facial Emotion Recognition*, 2021, p. 1.

roots in the work “Affective Computing” written by the computer scientist Rosalind Picard published in 1997. Starting from the assumption that both affect recognition and expression are a crucial psychological need of people, Picard coined the term affective computing defining it as “computing that relates to, arises from, or influences emotions”.[141] At the basis of her intuition lays the assumption that “if we want computers to be genuinely intelligent, to adapt to us, and to interact naturally with us, then they will need the ability to recognize and express emotions, to have emotions, and to have what has come to be called "emotional intelligence"”.[142]

Even though scholars do not unanimously agree on a single definition of the concept of emotion, the author clarifies how the numerous theories related to it share a cognitive as well as a physical dimension. While the cognitive component is mainly focused on examining the situations giving rise to emotions, the physical one focuses on the psychological responses accompanying an emotion. In fact, it has been determined how both body and brain cooperate in emotion generation processes, so that not only can thoughts generate emotions, but they can also be unconsciously aroused by changes in bodily chemistry without a cognitive evaluation being involved. As a result, according to affective computing in order to recognize and decode emotions, a computer has to be able to detect information by looking at one’s facial expression, tone of voice and gestures without the emotion being explicitly named and expressed. In this regard, it has been determined that the development of affective computers needs understanding of the physical component of emotion as well as the cognitive one.[143]

Furthermore, the concept of sentic modulation (encompassing voice inflections, posture and facial expressions which are one of the most widely recognized forms of it) has been defined as the set of physical traits through which emotions are typically expressed. In order to learn how to recognize human emotions, computers need to rely first and foremost on sentic modulation, rather than relying on people to explicitly state their emotions.[144] Eventually, three different types of affective computing applications are described.

---

[141] R.W. Picard, *Affective Computing*, M.I.T. Media Laboratory Perceptual Computing Section Technical Report No. 321, 1995, p. 1.
[142] R. W. Picard, *Affective Computing*, 1997, p. x.
[143] Ibidem.
[144] R.W. Picard, *Affective Computing*, M.I.T. Media Laboratory Perceptual Computing Section Technical Report No. 321, 1995, p. 22-26.

The first one refers to systems that detect the emotion of the user, the second relates to those systems expressing what a human perceives as an emotion and the last one refers to systems able to feel emotions.[145] For the purpose of this thesis only the system related to affect detection will be taken into consideration. It has been noted that affective detection poses many challenges[146] due to the nature of emotions, which are constructs with blurred boundaries and subject to individual variations in expression and experience.[147]

Despite this, it is widely assumed that it is possible to infer the emotional state of a person simply by looking at his face as there is a reliable and clear link between certain facial movements, referred to as expressions, and the emotions behind them. This commonly shared view lays at the basis of commercial applications, namely automated detection of emotions, in both government and industry. Not by chance, technology companies are prone to invest an extensive amount of resources in order to understand how emotions can be objectively read by means of detection of their facial expressions. An example is provided by Microsoft's Emotion API[148] claiming that it can determine how a person feels by analyzing video footage of one's face. More precisely, it explains that it can detect emotions like anger, contempt, disgust, fear, happiness, neutrality, sadness, and surprise, suggesting that these emotions are expressed in the same way across all cultures through specific facial expressions.[149] This reported example demonstrates how the common view of facial expressions tends to rely on six emotions categories[150] on which the great majority of studies on emotion perception have focused for decades.

---

[145] R. A. Calvo, S. D'Mello, *Affect Detection: An Interdisciplinary Review of Models, Methods, and Their Applications*, vol. 1, no. 1, 2010, p. 18.
[146] Limitations and challenges posed by emotion recognition systems as well as facial emotion recognition ones will be taken into consideration in the following sections of this chapter.
[147] Ibidem.
[148] "The Emotion API is a developer tool used to analyze faces and images to determine the emotional reaction to the stimuli." R. Deshmukh, V. Jagtap, *A Survey: Software API and Database for Emotion Recognition*, 2017, par. II Literature Survey.
[149] L. Feldman Barrett, R. Adolphs, S. Marsella, A. Martinez, S. D. Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, vol. 20, no. 1, 2019, p. 2,3.
[150] The common view related to emotions is rooted in the Basic emotion theory (BET) formulated in the article "*An Argument for Basic Emotions*" written by Ekman in 1992. In his study Ekman "detailed nine criteria to guide the scientific study of emotion: six differentiated emotions from related phenomena (moods, sentiments, traits); and three pointed to empirical approaches to differentiate distinct emotions from one another (in terms of antecedents, physiology, and signaling behavior)". D. Keltner, J.L. Tracy, D. Sauter, perA. Cowen, *What basic emotion theory really says for the twenty-first century study of emotion*, 2019**,** p. 1.

Alongside this, the Facial Action Coding System (FACS), developed by Ekman, has been presented as a systematic approach to describing the presence and intensity of facial movements through the detection of action units (AU's). Within this system AU should correspond to the contraction of a specific facial muscle corresponding to a specific facial movement. Such human coders need a lot of time and training before they can accurately assign AU codes. Even after they are trained, the process is still highly time-consuming as they have to go through images or videos frame by frame. This makes manual FACS coding impractical for analyzing facial movements in real-life situations. In this way, large collections of real-world photos and videos would take decades to be coded by hand. To overcome this obstacle automated FACS coding systems have been developed using computer vision techniques. As a result, these systems can identify and code a selected number of facial AU's, although they are not yet able to capture all of them.[151]

Scholars additionally clarify that the above-mentioned algorithms can reach remarkably high accuracy, around 99%, especially when they are trained and tested using images from the same dataset. Even when trained and tested on different datasets, they can still lead to good-quality results, with accuracy around 90%, as long as the images are collected in controlled, high-quality conditions. However, their performance tends to drop significantly when applied to real-world situations. When analyzing everyday photos or video frames, which present a varied and less predictable lighting, angles and facial expressions, their accuracy tends to significantly decrease compared to human FACS coding.[152]

Following the considerations reported above, it can be affirmed that in its early stages, affective computing was mainly based on predefined models in which emotional states were inferred through human-selected indicators, such as facial movements [153] or vocal inflections. However, recent fast-evolving advances in the field of artificial intelligence, and particularly the emergence of deep learning techniques, have deeply transformed emotion

[151] L. Feldman Barrett, R. Adolphs, S. Marsella, A. Martinez, S. D. Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, vol. 20, no. 1, 2019, p. 13, 14.
[152] Ibidem.
[153] As pointed out by Picard (1997) most facial expression recognition models have traditionally treated emotions as distinct categories, aiming to label expressions as specific feelings like "happy" or "angry." This approach is based on the already mentioned theory developed by Ekman, the Facial Action Coding System (FACS). In other words, the FACS system describes basic emotions and their corresponding sets of action units, which are muscular movements involved in the manifestation of a particular expression.

recognition systems, enabling models to autonomously learn complex representations from large-scale data. In addition to this, it should not be overlooked that progress in wearable technologies, mobile devices, and the Internet of Things (IoT) has enabled more efficient and diversified multidimensional applications for emotion monitoring.[154]

It is not by chance that over the last few years human-computer interaction has witnessed a progressive shift from a mere computer-centric approach to a progressively user-centered one. Indeed, starting from 2010, Deep Learning methods have been implemented and applied to affect recognition systems thus leading to an increase in their accuracy. Deep learning (DL) can be intended as a subset of machine learning (ML) falling within the broader field of artificial intelligence (AI) that aims to enable machines or systems to replicate aspects of human intelligence and behavior.[155]

Within this context, ML refers to methods that allow systems to learn from data or experience, leading to an automatization in the building process of analytical models. DL emerges as a class of these methods in which learning is performed through multi-layered neural networks. Indeed, the term "deep" highlights the presence of multiple processing layers, through which data is progressively transformed to construct data-driven models. Furthermore, deep learning not only takes AI to a higher level, known as Smarter AI, but it also makes a significant contribution to the development of technology-driven automation, as well as smart intelligent systems.[156] More specifically, deep learning systems rely on Deep Neural Networks (DNNs), whose design is inspired by biological neural networks. Thanks to their multiple layers of processing units (referred to as "neurons"), a well-trained Deep Neural Network can learn a hierarchical structure of distributed representations. This hierarchical organization allows the model to capture highly expressive features, enabling it to represent a wide range of possible input variations. One of the main advantages of deep architectures lies in their depth, as it facilitates the reuse of previously learned features.[157]

---

[154] R. Guo, H. Guo, L. Wang, M. Chen, D. Yang, B. Li, *Development and application of emotion recognition technology — a systematic literature review*, in *Frontiers in Psychology*, 2024, p. 2.
[155] P. V. Rouast, M. T. P. Adam, R. Chiong, *Deep Learning for Human Affect Recognition: Insights and New Developments*, 2021, p. 524.
[156] I. H. Sarker, *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, 2021, p. 3.
[157] P. V. Rouast, M. T. P. Adam, R. Chiong, *Deep Learning for Human Affect Recognition: Insights and New Developments*, p. 525.

2.2 Limitations and reliability of emotion recognition systems

Despite the increasing employment of emotion recognition systems in a wide range of contexts, the issue relating to their reliability remains controversial. While the previous section has outlined the theoretical foundations and functioning of affective computing systems, it is essential to assess the limitations that affect their accuracy and validity. Emotion recognition systems are not only limited by technical and methodological constraints. They are also deeply influenced by contextual, cultural and social factors, thus posing significant challenges in decoding emotional signals.

Particularly, the assumption that inner emotional states can be objectively inferred from detectable behavioral or physiological signals raises significant concerns, as emotions are highly context-dependent and cultural norms cannot be fully captured by standardized computational models. The above-mentioned limitations are further underlined by systematic biases embedded in data collection practices and algorithmic design, which may lead to unequal or discriminatory outcomes when applied on a large scale.

This section therefore examines the main technical limitations of emotion recognition systems, their context-dependent nature, and the risks related to cultural bias, setting the stage for the analysis of both ethical implications and social risks posed by such systems.[158]

As facial expression recognition (FER)[159] moved from controlled laboratory settings to more challenging in-the-wild conditions, it began to rely increasingly on deep learning techniques. Deep neural networks are widely used to learn effective representations for automatic FER. However, current approaches still face two major challenges. These concern, in the first instance, the risk of overfitting due to limited training data, and secondly, the presence of factors unrelated to facial expressions, such as lighting conditions, head pose, and identity-related biases.[160]

The combination of these variables and factors can negatively affect the performance of facial emotion systems. Although models based on basic emotions present limitations in grasping the complexity and subtlety of everyday emotional expressions, alternative

[158] The ethical implications and risks posed by the implementation of these technologies will be discussed in the next section of this dissertation.
[159] used in this section as a hypernym for facial emotion recognition.
[160] S. Li and W. Deng, *Deep Facial Expression Recognition: A Survey*, 2020, p. 1.

approaches, such as the Facial Action Coding System (FACS) and continuous dimensional models, offer a more detailed and flexible representation of affect. Nonetheless, the categorical model, which classifies emotions into a set of discrete basic categories, endures as the most widely used model in facial expression recognition due to its intuitive interpretation and deeply rooted academic foundations.[161]

More specifically, two broad categories of facial expression recognition (FER) have been identified based on their feature representations: namely, static image FER and dynamic sequence FER. Moreover, following 2013, emotion recognition challenges (for instance, FER2013 and Emotion Recognition in the Wild) have provided larger and more realistic datasets collected from real-world situations. This has allowed facial expression recognition research to migrate from controlled laboratory environments to more challenging in-the-wild settings. At the same time, major improvements in chip processing abilities and advances in neural network design have led to the implementation of deep learning methods, which have achieved significantly improved accuracy with respect to previous approaches. As a result, with more effective training data available, deep learning has increasingly been used to address the difficulties of recognizing emotions in real-world scenarios. Despite the powerful learning abilities of deep learning, several challenges remain when it is applied to FER. More specifically, deep neural networks require large amounts of training data in order to avoid overfitting. In relation to this aspect, it must be taken into consideration that current facial expression datasets are not large enough to effectively train deep architectures that have on the contrary shown excellent performance in other tasks such as object recognition. In addition, there is significant variation between individuals, as factors such as age, gender, ethnicity, and expressiveness can significantly influence how emotions are displayed.[162]

As previously mentioned, challenges such as Emotion Recognition in the Wild have pushed research toward less restrictive methods that can be applied in real-world settings. However, these approaches still rely on clearly visible and well-aligned faces, so that their performance decreases in quality when the face is occluded or not properly oriented toward the camera. Given the fact that deep learning systems highly rely on both data availability

[161] Ibidem.
[162] S. Li and W. Deng, *Deep Facial Expression Recognition: A Survey*, 2020, p. 2.

and quality, several datasets have been developed to address this limitation. However, it must be taken into consideration that each dataset has its own limitations and features, which can impair its execution ability in real settings. Limitations further extend to sample bias, as the data stored in the dataset does not accurately mirror the real-world conditions, and to recall bias, which arises from how multiple annotators are managed in the proposed scenarios. It can therefore be deduced that the main limiting factor is not related to the lack of computational resources or access to state-of-the-art deep learning models, but rather to the shortage of quality data needed to train them in an effective way. The design and crafting of a dataset is extremely expensive when considering specific tasks. This is particularly true for emotion recognition as it needs to create descriptions for concepts that are natural and innate to humans.[163]

In relation to this, a series of datasets have been examined as benchmarks for modern techniques.[164] Particularly, the Acted Facial Expressions in the Wild (AfeW) dataset was developed in order to solve the limitations imposed by the lack of data from real-word situations[165] by using scenes taken from movies containing environments similar to the real-world ones. Once the data has been extracted, two labelers annotate each sample with an expression. For each person present in the scene, the labels also contained information on the head pose, age of character, gender, and expression of the person. A further widely recognized dataset presented is the Emotions in Context (EMOTIC) whose aim was to collect images of subjects in their natural environments, including contextual information. The sample source used for EMOTIC relies on reused images from other datasets which are implemented with images taken from the web.[166]

A detailed analysis has identified a series of limitations concerning the above-mentioned datasets. iMiGUE, for instance, presents a simplified labeling scheme which reduces emotion understanding to merely "positive" or "negative" categories. In addition to this, its identity-free design, where facial details may be obscured for privacy, further limits

[163] W. Costa et al., *A Survey on Datasets for Emotion Recognition from Vision: Limitations and In-the-Wild Applicability*, 2023, p. 2,3.
[164] Such as the Context-Aware Emotion Recognition (CAER) dataset, the Body Language Dataset (BoLD), iMiGUE and GroupWalk.
[165] Originally, datasets were mainly composed of images recorded in laboratory scenarios with posed expressions.
[166] W. Costa et al., *A Survey on Datasets for Emotion Recognition from Vision: Limitations and In-the-Wild Applicability*, 2023, p. 6, 7.

the ability of models to learn richer emotional representations. As a result, its use is largely confined to narrow applications. Similarly, the GroupWalk dataset poses limitations related to data quality and image resolution. While varying camera perspectives can improve robustness, several footage appear to be unstable and of poor quality thus resulting in visual distortions. Low-quality samples and noise further affect the data. Additionally, the fact that bounding boxes[167] are embedded into the images can further lower the quality of the samples, despite common data augmentation[168] techniques like cropping and rotation. In conclusion, the field still lacks a sufficient number of datasets tailored to a wider range of specific real-world applications.[169]

A further limitation in this research area concerns how datasets are labeled. For instance, datasets such as EMOTIC and BoLD use a large set of 26 emotion categories but do not include a distinct neutral class, as they attribute labels like "Disconnection" or "Peace," which may overlap with neutral states. This design can introduce ambiguity, as visible cues from individuals may be associated with both positive and negative emotions, and the high number of classes can also reduce agreement between annotators. In contrast, datasets like CAER use a smaller set of seven categories, including a neutral class. Given their limited annotation structure, the attribution process of specific emotions to individuals is even more complicated, especially while considering settings when more people are present. Overall, there is also a lack of consistency across datasets in terms of label definitions and categories. These inconsistencies considerably limit their usefulness for specific applications, as some emotion classes which are available in one dataset may be missing in another.[170]

Lastly, an additional limitation concerns the lack of unanimous ontologies for emotion representation. Some datasets, for instance, describe "Surprise" as an emotion triggered by

[167] Bounding boxes are "usually defined as the minimal-area rectangle that encompasses the whole object region" J. Murrugarra-Llerena, L. Kirsten, C. R. Jung, *Can we trust bounding box annotations for object detection?*, 2022, p. 4813.

[168] Data augmentation can be defined as "a data-space solution to the problem of limited data. Data Augmentation encompasses a suite of techniques that enhance the size and quality of training datasets such that better Deep Learning models can be built using them." C. Shorten, T. M. Khoshgoftaar, *A survey on Image Data Augmentation for Deep Learning*, 2019, p. 1.

[169] W. Costa et al., *A Survey on Datasets for Emotion Recognition from Vision: Limitations and In-the-Wild Applicability*, 2023, p. 19, 20.

[170] Ibidem.

unexpected events that can have either positive or negative evaluations, a distinction that is usually not captured in existing datasets. Similarly, datasets evaluate emotions such as "Happiness" and "Pleasure" as being closely related, while others suggest that "Pleasure" may be linked to broader states such as satisfaction, offering a more nuanced interpretation.[171]

The scarcity of data discussed above is not merely quantitative, but also qualitative. Indeed, it has to be considered that the majority of current work in affective computing relies on emotion representation schemes that avoid dealing with ambiguity in perceived emotions. Even if a few studies consider ambiguous or uncertain emotion representations, they are still limited by the lack of clearly established methods for evaluating accuracy and making comparisons between each other. This issue largely stems from the absence of a shared and standardized language for describing emotions. A further critically relevant point to highlight is that most systems are not designed to manage ambiguity in emotional expression. As a result, they are unable to properly interpret or respond to emotions that appear uncertain or unclear. This leads to significant limitations, as such systems may hinder their deployment in real-world applications if they cannot handle the full range of human emotional expression, or if they attempt to make definitive judgments about underlying emotional states when such certainty is neither justified nor possible.[172]

As early as 2017, it was pointed out that the limitations affecting even the most advanced architectures have not yet been fully overcome, as they stem not from computational constraints but rather from the unpredictability of human posture and environmental conditions. Research indicates that upper cameras tend to overestimate anger (as eyebrows are recorded from upper perspective, they appear lower than in zero angle position), while lower ones seemed to overestimate surprise, as eyebrows are recorded from a lower perspective, so that they appear to be positioned higher than in the neutral zero-angle position. While summarizing the results it is observed that "all automatic emotion recognition algorithms are susceptible to some disturbances and facial expression analysis

[171] Ibidem.
[172] V. Sethu et al., *The Ambiguous World of Emotion Representation*, 2019, p. 3,6.

is not an exception – suffers from face oval partial cover, location of the camera, insufficient or uneven illumination". In a nutshell, an alarming rate of inconsistency is identified.[173]

The technical limitations of FER have also been identified in studies examining the commercial application of AI and facial expression recognition systems in the retail sector. The preliminary assumption is that digital developments have brought substantial challenges to brick-and-mortar stores and traditional retailers. To remain competitive, a growing number of physical retail stores are adopting technologies such as AI and the Internet of Things (IoT) to detect and decode customer behavior and emotions. These tools can allow retailers to turn data into meaningful insights, thus leading to an improvement in the in-store shopping experience while supporting business decision making. Findings from studies in this field suggest that combining multiple advanced models can significantly improve facial expression recognition in retail business intelligence applications. In particular, the adopted ensemble approach outperformed traditional single-model methods, achieving high validation accuracy (86.93%). Nonetheless, the study uncovered several limitations. Although the model operated efficiently in recognizing "Happy" and "Neutral" emotions, its accuracy decreased for more complex categories such as "Disgust," "Fear," and "Sad." This indicates that emotions with similar or overlapping facial features are more difficult to be distinguished by the model. Furthermore, the latter frequently presented confusion while differentiating between "Fear" and "Surprise," as well as between "Disgust" and "Angry," thus suggesting a struggle in capturing subtle differences in facial expressions.[174]

While discussing facial emotion recognition systems, the prominence of context cannot be overlooked, as it is a key factor in both determining and decoding facial expressions and, consequently, an individual's emotional state. However, it is widely believed that specific facial movements match with particular emotional states, meaning that a person's face can be used to directly infer what they are feeling. This traditional view

[173] A. Landowska, G. Brodny and M. R. Wrobel, *Limitations of Emotion Recognition from Facial Expressions in e-Learning Context*, 2017, p. 388.
[174] C. Qian and J. A. Lobo Marques, *Consumer Response Analysis with AI and Facial Expression Recognition in Retail*, 2025, p. 351,352.

persists despite the agreement among many scholars that emotional expressions are far more variable and strongly context dependent.[175]

Despite a growing scientific consensus in this respect, the assumption of a fixed link between facial expressions and emotions continues to influence multiple domains. As has been clearly established "this common view continues to fuel commercial applications in industry and government (e.g., automated detection of emotions from faces), guide how children are taught (e.g., with posters and books showing stereotyped facial expressions), and impact clinical and legal applications".[176]

Three major limitations in the scientific study of facial expressions have been subsequently identified, which have contributed to widespread misunderstandings regarding how emotions are expressed and interpreted. The first point is related to limited reliability, as instances of the same emotion category are not consistently expressed or recognized through a common set of facial movements. The second point concerns the lack of specificity, as no unique and direct correlation exists between a particular facial configuration and a specific emotion. In other words, the same pattern of facial movements can be associated with different emotional states, thus undermining the idea that every emotion is marked by precise and univocal signals. Lastly, the limited generalizability is taken into consideration. Research findings often fail to account for the influence of context and cultural variations. As a result, conclusions drawn from controlled or culturally narrow studies may not suit real-world settings, where emotional expression and perception are shaped by situational and cultural factors.[177]

Considering this, it has been postulated that only when a pattern of facial muscle movements perfectly fulfills a set of specific criteria[178] one can consider it to be an emotional expression. A further challenge is posed by the issue of validity, which is rarely addressed in studies of emotional expression and perception. Even considering instances where facial movements appear to be reliable, specific, and generalizable, it remains an

[175] L. Feldman Barrett, R. Adolphs, S. Marsella, A. Martinez, and S. D. Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 2019, p. 2
[176] Ibidem.
[177] Ivi p. 5.
[178] Namely reliability, specificity, generalizability and validity.

open and unresolved question whether such movements can legitimately support inferences[179] about a person's actual emotional state.[180]

In other words, observing a particular facial configuration does not necessarily provide valid evidence of what someone is truly feeling. One's brain can be indeed influenced by multiple factors. For instance, emotional expressions, such as anger, can vary substantially depending on a wide range of influencing factors: namely situational context (for example whether a person is at work, school, or home), social context (such as who is present and the relationship between individuals), and internal physical states (e.g., fatigue or hunger). Additionally, internal mental processes, including past experiences and personal evaluations, considerably shape how emotions are expressed. Temporal factors (what have just occurred), individual differences (such as personality traits or gender), and cultural context also play a fundamental role. For instance, expressions may differ across cultures that prioritize individual autonomy versus those that emphasize group harmony, or between more permissive versus more norm-driven social environments. All in all, this variability underscores that emotional expressions are neither fixed nor universal, but rather dynamically shaped by the merging of contextual, personal, and cultural factors.[181]

Research findings indicate that facial configurations are not to be intended as "fingerprints" of emotions. Instead of being diagnostic displays, they constitute highly variable signals that cannot reliably indicate specific emotional states without accounting for context, individual differences, and culture. In conclusion, it is not possible to infer happiness with certainty merely from a smile, anger from a scowl, or sadness from a frown. Such simplified interpretations fail to adequately account for the variability and context-dependence of emotional expression. Despite this, many technological applications continue to rely on this mistaken assumption, treating facial movements as objective

[179] With respect to emotional inference Barrett et al. (2019) state that "When you see someone smile and infer that the person is happy, you are making what is known as a reverse inference: you are assuming that the smile reveals something about the person's emotional state that you cannot access directly. […] Reverse inference requires calculating a conditional probability: the probability that a person is in a particular emotion episode (such as happiness) given the observation of a unique set of facial muscle movements (such as a smile). L. Feldman Barrett, R. Adolphs, S. Marsella, A. Martinez, and S. D. Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 2019, p. 8.
[180] L. Feldman Barrett, R. Adolphs, S. Marsella, A. Martinez, and S. D. Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 2019, p. 8, 9.
[181] Ivi p. 10.

evidence of internal emotional states, despite the lack of solid scientific support for such claims.[182]

Building on the analysis and the critique outlined above, recent academic literature shows that context-dependency and theoretical uncertainty persist even when emotion recognition relies on physiological signals rather than facial expressions. Indeed, a systematic literature review highlights that datasets for physiological signals remain limited, particularly those combining physical and physiological data. In addition, standardized methods for collecting and building these kinds of datasets have not yet been clearly defined.[183]

It has been observed that there is still much to be done in the study of emotions using body-based indicators, which are currently largely limited to controlled laboratory settings. At the same time, there is a growing shift toward the use of non-intrusive sensors and wireless technologies, enabling data collection in real-world environments and offering more relevant insights into everyday emotional experiences. Even if there have been significant improvements in developing smaller and portable devices, they are still more intrusive than everyday wearable technologies such as smartwatches, which many people are used to wearing regularly. As a result, developing systems that rely on non-intrusive devices while achieving the same level of performance as EEG-based methods[184] remains a major challenge. However, the major limitation for this development lies in the very nature of human physiological signals, as they vary significantly between individuals making it difficult to standardize them for broad-spectrum applications. Moreover, processing and interpreting this type of data is a complex process which requires advanced algorithms to accurately extract meaningful information. Lastly, creating reliable and representative datasets requires large participant samples in order to properly capture differences between individuals.[185]

---

[182] Ivi p. 49.
[183] R. A. García-Hernández, H. Luna-García, J. M. Celaya-Padilla, A. García-Hernández, L. C. Reveles-Gómez, L. A. Flores-Chaires, J. R. Delgado-Contreras, D. Rondon, and K. O. Villalba-Condori, *A Systematic Literature Review of Modalities, Trends, and Limitations in Emotion Recognition, Affective Computing, and Sentiment Analysis*, in *Applied Sciences*, 2024, p. 20.
[184] "Electroencephalography, or EEG, is a powerful non-invasive technique that captures the electrical activity of the brain". Healthy Mind, *Neuromind: The Alliance of Neuroscience and AI*, 2026, https://healthymind.fr/en/solution-neuromind/, accessed 14 April 2026.
[185] R. A. García-Hernández, H. Luna-García, J. M. Celaya-Padilla, A. García-Hernández, L. C. Reveles-Gómez, L. A. Flores-Chaires, J. R. Delgado-Contreras, D. Rondon, and K. O. Villalba-Condori, *A Systematic*

In light of the above considerations, findings suggest that even when alternative signals and architectures are adopted, emotion recognition remains inherently restricted, especially when moved from controlled environments to real-world and generalized applications. In addition to technical and methodological limitations, emotion recognition systems face a further fundamental limitation related to cultural differences in the expression and interpretation of emotions. Before examining the role of cultural factors in the expression of emotions, it is necessary to clarify what is meant by "culture". A widely recognized definition is provided by Hofstede who describes culture as ""the collective programming of the mind that distinguishes the members of one group or category of people from others". It is always a collective phenomenon […] [and] can also be applied to the genders, to generations, or to social classes."[186] In particular, six dimensions for the analysis of cultural differences have been identified, focusing on how societal values influence behavior across different societies.[187]

The application of Hofstede's dimensions to the notion of emotion expression, particularly Individualism versus Collectivism and Power Distance, can offer a useful framework to ponder some of the challenges faced by automated emotion recognition systems. To give an example, in individualistic societies, emotions may be interpreted and valued as a display of authenticity, whereas in collectivistic cultures, the modulation or suppression of certain facial movements may be preferred in order to preserve social harmony. Similarly, in high power distance contexts, emotional displays are subject to a strict hierarchical order, so that the manifestation of certain emotions (such as anger toward a superior) is socially discouraged.

The theoretical framework provided by Hofstede finds empirical support in studies that challenge the universality hypothesis according to which all humans communicate six

---

Literature Review of Modalities, Trends, and Limitations in Emotion Recognition, Affective Computing, and Sentiment Analysis, in *Applied Sciences*, 2024, p. 20,21.

[186] G. Hofstede, *Dimensionalizing Cultures: The Hofstede Model*, 2011, p. 3.

[187] "The six dimensions are labelled as: 1. *Power Distance*, related to the different solutions to the basic problem of human inequality; 2. *Uncertainty Avoidance*, related to the level of stress in a society in the face of an unknown future; 3. *Individualism* versus *Collectivism*, related to the integration of individuals into primary groups; 4. *Masculinity* versus *Femininity*, related to the division of emotional roles between women and men; 5. *Long Term* versus *Short Term Orientation*, related to the choice of focus for people's efforts: the future or the present and past. 6. *Indulgence* versus *Restraint*, related to the gratification versus control of basic human desires related to enjoying life." G. Hofstede, *Dimensionalizing Cultures: The Hofstede Model*, 2011, p. 8.

basic internal emotional states[188] by displaying the same facial movements on the basis of their biological and evolutionary origins.

The cross-cultural comparisons of mental representations have significantly challenged the universality stance. Particularly, it has been observed that, while Westerners share a common representation of the six basic emotions based on a distinctive set of facial movements, Easterners do not. Additionally, they represent emotional intensity with distinctive dynamic eye activity. Data shows that the six basic emotion framework is inadequate and cannot be extended to East Asian culture, where fundamental emotions such as pride, shame or guilt are likely to be neglected. While Caucasians represent the six basic emotions with a distinctive set of facial muscles, East Asian models showed a lower degree of distinction. They are characterized in fact by a significant overlap between emotions categories (particularly when considering surprise, fear, disgust or anger). In other words, cross-cultural analysis revealed culture-specific differences in both where on the face and when facial expressions communicate emotional intensity. In light of this, it has been argued that, although basic facial expressions such as fear and disgust were originally adaptive responses in early human evolution stages, facial expressions have developed over time and diversified becoming powerful tools exploited to convey emotions in an increasing variety of communication contexts. Consequently, such once innate and universal signals have been accordingly shaped and modified by the different cultural beliefs and social practices of the groups using them.[189]

To further reinforce the evidence against universality, valuable insights have been provided by studies that shift the perspective by focusing on remote cultural contexts. By comparing participants from the United States with those from the Himba ethnic group in Namibia, it has been demonstrated that the perception of facial expressions is not deeply rooted in a universal biological code, rather it is heavily influenced by cultural and linguistic exposure. Participants from the United States and the Himba ethnic group were asked to categorize images of posed facial expressions according to their perceived emotion type. Without being given explicit emotion cues, Himba participants did not line up with the expected universal classification pattern, whereas participants from the United States

[188] Namely happy, surprise, fear, disgust, anger, and sad.
[189] R. E. Jack, O. G. B. Garrod, H. Yu, R. Caldara, and P. G. Schyns, *Facial expressions of emotion are not culturally universal*, 2012, p. 7241, 7242.

showed responses more closely aligned with it. However, when provided with emotion-related cues, individuals from both cultural groups produced categorizations that more closely approximated the presumed universal pattern, although significant cultural variability persisted. The research concluded that in the absence of emotion concepts to guide their perception, Himba individuals tended to interpret facial expressions as observable behaviors without necessarily associating them with a specific emotion. In contrast, participants from the United States were more likely to perceive these expressions in mental terms, aligning them with the presumed universal categories of emotion.[190]

A further significant finding emerging from the above-presented research is that, when emotion-related words were introduced, participants from both cultures altered the way in which they grouped facial expressions. U.S. participants showed a clearer shift toward the commonly assumed "universal" pattern, whereas in Himba participants only subtle changes occurred. Although emotion words appeared to align participants' perception toward more standardized categories, the results did not fully comply with the universal model. In conclusion, findings suggest that emotion perception is influenced by both language and its culture of belonging. Even when emotional words are shared across different languages, people from unrelated cultural backgrounds do not necessarily interpret emotional expressions in the same way, so that their internal mental representations of emotions remain culturally specific.[191]

This evolutionary diversification further explains why automated systems, when designed without accounting for cultural nuances and variabilities, inevitably face a significant drop in accuracy and validity, thus questioning their suitability for generalized or large-scale deployment. The structural unreliability and contextual dependency of emotion recognition systems are therefore particularly relevant when assessing their compatibility with the right to private life under Article 8 ECHR, as they expose individuals to misinterpretation and classification of sensitive and intimate aspects of individuals' interiority.

[190] M. Gendron, D. Roberson, J. M. van der Vyver, and L. Feldman Barrett, *Perceptions of Emotion From Facial Expressions Are Not Culturally Universal: Evidence From a Remote Culture*, in *Psychological Science*, 2014, p. 251.
[191] Ivi p. 259.

2.3 Ethical implications and social risks related to emotional recognition systems

The technical and methodological limitations discussed in the previous section of this chapter strongly suggest that emotion recognition systems lack the proportionate level of reliability required for both emotion decoding and objective affective inference. As contextual influence and cultural variables play a crucial role in how emotions are perceived, expressed and classified emotional displays cannot be recognized as universal fingerprints. Considering this it can be affirmed that such technologies operate in a minefield as they are subject to inevitable biases and approximations posed by technical limitations. However, the implications of these deficiencies extend far beyond technical inaccuracies, thus posing significant ethical and social concerns. When systems characterized by such a level of validation deficits are applied to real-world contexts, such errors translate into concrete risks of discrimination and, ultimately, into potential infringements of individual autonomy. In this regard, the present section examines the ethical implications of deploying emotion recognition models, with particular attention to the risks of systematic bias, the intrusion into privacy through affective surveillance, and the potential use of these tools as mechanisms of social sorting in sensitive domains such as public security and consumer environments.

As a starting point it must be recognized that emotion recognition systems are applied to various fields. Within the context of marketing and advertising, for instance, it is deployed to assess consumers' emotional responses to products and promotional contents with the aim of developing the customization of more tailored and personalized strategies. Similarly, in healthcare they can assist professionals in tracking patients' emotional states with the aim of formulating accurate diagnoses thus enabling targeted therapeutic procedures. When applied within the educational contexts, emotions recognition systems can help evaluate students' level of engagement so that approaches to enhance learners' outcomes can be accordingly adjusted. Another example is provided by the employment sector, where these technologies have been explored as a tool for determining employees' well-being, including satisfaction, stress and productivity.[192]

[192] J. N. Nartey, *The Ethics of Emotion Recognition Technology: Implications for Privacy and Consent*, 2023, par. II. Overview of emotion recognition technology.

However, despite its potential advantages, the implementation of such systems raises significant ethical concerns, among which privacy and data protection are the most critical points. Emotional data gathered through emotions recognition technologies represents a sensitive data category, as it provides insight into an individual's psychological state. The misuse or exploitation of such data can thus lead to serious repercussions, including emotional manipulation, discrimination, and loss of privacy. Consequently, it is essential to implement reliable data storage and management systems in order to ensure adequate protection of emotional information against unauthorized access and misuse. Informed consent and transparency pose further risks, as obtaining meaningful consent for emotion detection can be challenging. Individuals cannot fully grasp the implications related to the sharing of their emotional data or its potential use. Additionally, the increasing implementation of these systems in everyday environments may inhibit individuals from withdrawing from or checking the collection of such data.[193]

In studies examining the influence of race on automated perceptions of emotions, it has been observed that, in the field of human resources, some organizations have adopted video-based hiring platforms to screen candidates. Applicants had to answer predefined questions by recording a video so that organizations can use facial expression recognition systems to analyze the potential applicant faces. The outcomes of such analyses can consequently influence recruitment decisions. Similarly, within the context of threat detection, companies are developing facial recognition systems to monitor crowds in order to assess whether individuals may be a risk for public safety. For instance, the company WeSee claims that its technology can infer one's mental state by detecting expression hints not directly observable by solely human scrutiny. This approach often focuses on identifying emotions such as anger or doubt, which are interpreted as potential indicators of threatening behavior. In both scenarios, the deployment of facial emotion recognition systems can lead to significant consequences for individuals. If an AI system incorrectly interprets a candidate's facial expression as anger during a job interview, he may be unfairly excluded from being considered for the job position he applied for, thereby limiting his career opportunities. Likewise, an inaccurate classification in the context of security and

[193] Ivi. Par. III. Ethical concerns surrounding ERT.

surveillance of an individual as a potential threat may result in severe actions such as surveillance, detention, placement on no-fly lists, or other restrictive measures.[194]

Research in this field has demonstrated that facial recognition systems may interpret emotional expressions differently depending on an individual's ethnic group. Using a dataset of professional basketball players' pictures, a comparative analysis was conducted between the outputs of two facial recognition platforms, namely Face++ and Microsoft AI. The findings indicate that both systems are prone to attributing more negative emotions to black players than to white ones, with the nature of this bias varying across the platforms. On the one hand Face++ consistently classifies black players as angrier than their white counterparts, even when examining variations in smiling. On the other hand, Microsoft's system is more likely to assign expressions of contempt rather than anger, particularly when facial expressions are ambiguous.[195]

The above-mentioned findings are further supported by more recent research that takes into account the decade between 2014 and 2025, the conclusions of which provide consistent evidence. Namely, a considerable number of AI systems tend to reproduce or even intensify already existing racial and ethnic inequalities across different domains. In healthcare, for instance, these systems often show lower accuracy and higher error rates when applied to black, latino, and indigenous populations. Comparably, in security and criminal justice contexts, AI technologies tend to generate disproportionately higher rates of false positives for minority groups, raising concerns about fairness and equity. Even when considering commercial facial recognition systems, higher error rates emerged in the identification of non-white skin faces compared to Caucasian ones, as a result of training data disproportionally focused on white faces. Even the legal field is not immune from these risks, as predictive models of criminal risk systematically scored African American defendants as more likely to repeat the offence with respect to white ones while facing equivalent situations.[196]

Such discrepancies are often attributed to unbalanced representation within datasets, including insufficient samples of minority groups and the presence of embedded historical

[194] L. Rhue, *Racial Influence on Automated Perceptions of Emotions*, 2018, par. Introduction.
[195] Ibidem.
[196] J. S. Fernández-Prados, Y. Cara-Fernández, M. J. Torres-Haro, *Racial/Ethnic Bias in AI Systems: A PRISMA Systematic Review of Magnitude, Domains, and Mitigation Strategies (2014–2025)*, 2025, p. 58,59.

biases. However, more recent studies point out the way in which models are trained, the design choices made during their development (namely included or excluded variables) as well as the specific contexts in which these systems are deployed significantly contribute to the persistence of bias. Even when datasets are balanced, bias can still emerge. A primary example is provided by models optimized through evaluation metrics that do not account for fairness, thus overlooking the examination of how errors are distributed across different groups of people. In addition to this, interaction bias may arise when dissimilar user groups interact with AI systems in different ways (for instance, by posing different types of queries to a virtual assistant), thus ultimately leading to uneven or biased system results.[197]

Within this framework, the concepts of "data colonialism" and "digital colonialism" have become increasingly prominent among academics, policymakers and organizations who criticize harmful AI practices. The concept of colonialism is thus used to highlight the extractive and exploitative means used to subjugate people to the will of technological companies. In Europe, for instance, this term lies at the basis of groups who advocate decentralized and community-owned-data governance mechanisms. Within the context of open-data movements, several indigenous-led movements advocating sovereignty and data self-determination have gained ground. The Indigenous Data Sovereignty program was established to not only address the limited availability of reliable data and information about indigenous people, but also to face the inappropriate use of their traditional knowledge and cultural heritage. Particularly, the term "indigenous data sovereignty" generally defines the right of a nation to collect, dispose of and implement its own data. Not by chance the concept of data colonialism is currently used even by non-indigenous policy and advocacy groups to exercise the right to object to data processing and ownership policies.[198]

Following the publication of several studies, significant performance disparities across intersectional demographic subgroups persist in commercial facial-recognition products. To cope with these limitations, some companies have attempted to mitigate bias by increasing the diversity of their training datasets. However, a mere dataset diversification is far from being the solution to mitigate the concerns surrounding the use of facial and

[197] Ivi p. 64.
[198] K. Crawford, R. Dobbe, T. Dryer, G. Fried, B. Green, E. Kaziunas, A. Kak, V. Mathur, E. McElroy, A. Nill Sánchez, D. Raji, J. L. Rankin, R. Richardson, J. Schultz, S. Myers West, M. Whittaker, *AI Now 2019 Report*, 2019, p. 43,44,45.

emotional recognition systems. Facial datasets are indeed a collection of artifacts, whose composition reflects a series of decisions about who is included and excluded.[199]

A further concern is aroused by scholars regarding the sensitivity of emotions when collected as data. Since the boundaries between whether an expression is considered to fall within the public or private scope are blurred and context dependent, its collection may lead to an invasion of the individual sphere. Moreover, intelligent systems are increasingly fed with biometric data with the aim of improving user experience. However, constant predictions and analysis of human behavior may place fundamental rights at risk, thereby creating new forms of power and control. An example is provided by applications that claim to enhance the quality of life for people with disabilities. This further fuels ethical questions, as such systems may also contribute to the exploitation of clinical conditions to foster rhetoric aimed at promoting surveillance capitalism. A case in point is Affectiva's Affdex[200], in which autism is exploited as a justification for turning emotions into computationally measurable units, thereby supporting the advancing of commercial emotion AI.[201]

In the era of affective computing, emotions have begun to be quantified so that they can be assigned an economic value. The relevance of this process is articulated through five main points that can be summarized as follows. In the first place, expressions of subjectivity in public spaces are increasingly appropriated, contributing to the datafication and extraction of aspects of human experience that were previously considered beyond the scope of commercial exploitation. As a result, subjective human experiences are transformed into objects that can be measured, analyzed, and manipulated.[202]

Ultimately, unlike many other digital interactions where personal data is knowingly exchanged, this form of reciprocal exchange is absent in the data mining of public emotional life. In this context, it has been argued that legal, regulatory, and governance mechanisms

[199] Ivi p. 52.
[200] "AFFDEX 2.0 [is] a toolkit for analyzing facial expressions in the wild, that is, it is intended for users aiming to; a) estimate the 3D head pose, b) detect facial Action Units (AUs), c) recognize basic emotions and 2 new emotional states (sentimentality and confusion), and d) detect high-level expressive metrics like blink and attention. AFFDEX 2.0 models are mainly based on Deep Learning and are trained using a large-scale naturalistic dataset consisting of thousands of participants from different demographic groups." M. Bishay, K. Preston, M. Strafuss, G. Page, J. Turcot, M. Mavadati, *AFFDEX 2.0: A Real-Time Facial Expression Analysis Toolkit*, 2022, par. Abstract.
[201] M. Mattioli, F. Cabitza, *Not in My Face: Challenges and Ethical Considerations in Automatic Face Emotion Recognition Technology*, 2024, p. 2220.
[202] A. McStay, *The Right to Privacy in the Age of Emotional AI*, 2020, p. 3.

have so far been effectively bypassed. This is largely due to the overemphasis on individual privacy within current regulatory frameworks, which focus exclusively on the rights of the single subject while neglecting the collective dimension. By overlooking the collective dimension of affective surveillance, current frameworks fail to protect the public sphere from the systemic extraction and categorization of emotional states, thus making the communities vulnerable to algorithmic governance.[203]

For these reasons, the commodification of emotions requires careful and critical consideration. The objective should not be to ban emotion-recognition technologies, but rather to develop ways of integrating them into society while simultaneously preserving human dignity and prioritizing the well-being of individuals over exploitation. In this respect, a number of concrete risks has been identified as emerging when emotional data are extracted and processed without adequate safeguards:

> "4.2.2 People are seen as objects rather than as subjects.
>
> 4.2.3 People do not have control over sensitive information collected from them.
>
> 4.2.4 Passive tracking collects intimate data without consent.
>
> 4.2.5 Alienation of citizenry from public spaces.
>
> 4.2.6 Unwanted attention to behaviour and the body.
>
> 4.2.7 Increased scope to manipulate consumer behaviour through application of behavioural sciences.
>
> 4.2.8 Abuse of dignity."[204]

All things considered, the above-discussed ethical challenges posed by emotion recognition systems pierce the very heart of fundamental human rights. As outlined in the first chapter of this dissertation, Article 8 ECHR aims at providing robust protection for the individual, by safeguarding one's personal autonomy, identity and privacy. At the core of

[203] Ivi p. 4.
[204] Ivi p. 6.

this protection lies the right to a private sphere, which grants that the most intimate aspects of an individual remain sheltered from unauthorized external scrutiny and unjustified interference. From this perspective, emotion recognition could constitute one of the most invasive forms of technological interference with the right to privacy protected by Article 8 ECHR, as it relates to aspects of personal identity that are not necessarily externalized or deliberately expressed.

The deployment of ever-advancing technologies within the field of affective computing may result in actual disproportionate interferences with the inalienable human rights enshrined by the provisions entailed within the European Convention on Human Rights. By attempting to decode, categorize and commercialize human emotional states, these systems pose a concrete threat to the most intimate and inner sphere of the individual, potentially jeopardizing the free development of one's personality and individual autonomy. Consequently, an imperative need to effectively translate the principles of Article 8 ECHR into the digital age has gradually emerged, paving the way for more robust and comprehensive legal measures.

The following section will therefore consider the tangible actions adopted to implement the European legal framework. This implementation aims to regulate AI-powered technologies, particularly emotion recognition systems, in order to ensure that human dignity and fundamental rights are not sacrificed in the name of economic benefits and technological innovation.

2.4 The EU Artificial Intelligence Act: a regulatory response to emotion recognition systems

As discussed in the previous sections of this chapter, over the past few years AI-powered systems have started reshaping individual lives and interactions, as well as economic and political organizations. Considering this, the development of appropriate policies and regulations related to AI turned out to be a pressing priority for the European Union. It is undeniable that AI brings significant opportunities across different domains by fostering economic development, healthcare and knowledge production. At the same time,

however, it poses serious challenges including the risk of job displacement, biases and social exclusion.

For this reason, it is essential not only to promote research and innovations in the field of AI, but also to implement a robust legal framework and ethical guidelines grounded in European values of inalienable and fundamental human rights. Such measures should ensure that AI serves the broader public interest at its best. The goal is therefore to promote a balanced approach so that AI is employed in ways that comply with human dignity while enhancing human capabilities. Both underutilization of AI systems as well as excessive or inappropriate use of the latter should be avoided, as it could lead to negative side-effects.[205]

In particular, the combination of AI and data processing can pose significant risks to individuals. For instance, profit-making actors may use AI to pursue economic objectives in ways that can harm individuals. They may indeed subject users to pervasive surveillance, thus narrowing the scope of choices and information available to them. Additionally, they can influence consumers' decisions in ways that do not align with their best interests. It has been argued that "[…] we need to focus not only on existing regulatory frameworks, but also on first principles, given that the available rules may fail to provide appropriate solutions and direction to citizens and legal decision-makers. First principles include fundamental rights and social values at both the ethical and the legal level".[206]

A comprehensive synthesis of the ethical framework for AI systems has been developed, balancing potential opportunities with the corresponding risks. While AI can enable human self-realization, it can accordingly devalue human abilities. It can enhance human agency on the one side, while removing human responsibility on the other. Lastly it can increase both societal capabilities and cohesion, while reducing human control and self-determination.[207]

Shifting from the ethical to the legal dimension, artificial intelligence is able to promote but also to undermine the set of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. These include not only the right to human

[205] G. Sartor, *Artificial Intelligence: Challenges for EU Citizens and Consumers*, 2019, p. 2.
[206] Ivi p. 4.
[207] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke e S. Vayena, *AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, 2018, p. 10.

dignity, freedom of thought, conscience, and religion, but foremost the right to privacy and data protection. Given the legally binding nature of the EU Charter of Fundamental Rights, it provides a foundation not only for lawful AI, but also for ethical AI, thus considering the inherent moral status of every human being. In this regard, particular emphasis has been placed on the importance of legal safeguards to address asymmetries within consumer markets, where emotional AI may be exploited to influence and distort individuals' decision-making processes.[208]

Taking into account the above-mentioned risks, the High-Level Expert Group on Artificial Intelligence (AI HLEG) developed guidelines with the aim of promoting Trustworthy AI. This concept lies its basis on three main components that must be ensured throughout the entire lifecycle of a system. In the first instance, AI must be lawful, in order to comply with applicable laws and regulatory requirements. Secondly, it should be ethical, by adhering to established ethical principles and societal values. Lastly, it needs to be technically and socially robust, since, even with good intentions, AI systems can cause unintentional harm. To sum up, the guidelines are intended to "ensure that the development, deployment and use of AI systems meets the seven key requirements for Trustworthy AI: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability."[209]

Even though the European Union has already developed a consistent legal framework aimed at safeguarding fundamental human rights in the digital era, these legal instruments have progressively revealed limitations while facing the fast-paced development and deployment of AI systems. As extensively discussed in the first chapter of the present dissertation, GDPR provides for instance, a robust instrument for the safeguard and the processing of personal data, grounded in principles such as lawfulness, transparency, purpose limitation and accountability. Nevertheless, it was primarily developed to focus on data protection rather than on the broader risks generated by AI-driven systems.

[208] R. Pusztahelyi, *Emotional AI and its Challenges in the Viewpoint of Online Marketing*, 2020, p. 15.
[209] High-Level Expert Group on Artificial Intelligence (AI HLEG), *Ethics Guidelines for Trustworthy AI*, European Commission, 2019, p. 2.

In particular, the GDPR was not designed to address the advanced technical features of artificial intelligence, such as autonomous learning, opacity, and the ability to infer sensitive human features beyond the data previously collected. As a result, significant risks related to algorithmic bias, manipulation, profiling, and interference with individual autonomy and private life may endure even in the presence of GDPR compliance, thus posing significant challenges to privacy preservation. Such regulatory gaps have become strikingly obvious in relation to AI technologies, such as emotion recognition systems, whose functioning goes beyond the mere processing of personal data and extends to the prediction, classification, and evaluation of human behaviors and subjective traits. As will be considered in the next paragraphs of this section, this shift prompted by new tools inevitably determines a transition from a data-centric regulation to a risk-based approach.

According to Article 9 of the GDPR, emotional data is not explicitly classified as a special category of personal data, despite its sensitive nature and the potential impact of its processing on individuals. Such controversy may generate uncertainty for developers operating in the field of affective computing. Indeed, under the GDPR, the processing of special data categories is generally prohibited unless specific derogation applies. Whether emotion data falls into this category depends on the method of collection. If such data are derived from physiological signals (such as heart rate or brain activity), they are considered a special data category and are therefore subject to strict limitations. By contrast, approaches based on the visual analysis of facial expressions do not qualify as a special category of personal data.[210]

Even though emotions are perceived as personal traits, as they are related to individual values, from a legal perspective, they are not automatically regarded as personal data. More specifically, processing emotion data does not fall under the material scope of the GDPR in case an individual is neither identified nor identifiable. Techniques such as sentiment analysis of text, emotion detection from audio, or recognition of facial expressions and body movements do not directly involve sensitive personal data as defined in GDPR provisions. Even the emotional information derived from these methods is not necessarily classified as a special data category. This is also the case when biometric signals are used to infer

[210] A. Häuselmann, E. Fosch-Villaronga, A. M. Sears, L. Zardiashvili, *EU law and emotion data*, 2023, par. I Introduction.

emotions. An example is provided by automated facial analysis based on FACS, as its primary aim is not to identify a subject, but rather to interpret facial expressions. Similarly, systems deployed to analyze voice or speech in order to collect emotional cues are not, as such, considered to process special category biometric data. Under Article 9(1) of the GDPR, biometric data is classified as a special category of personal data only when it is processed for the purpose of uniquely identifying an individual, and not when it is used solely for emotion recognition.[211]

In order to effectively address the limitations and gaps set by the existing regulatory plan, the EU Commission proposed a more comprehensive and innovative regulatory response specifically designed to address the challenges posed by artificial intelligence, namely the Artificial Intelligence Act (AI Act). It was officially published in July 2024 while in August 2024 it entered into force as the first comprehensive framework on AI on a global scale. However, the AI Act legislative process started in 2021, proving its drafting to be far from linear, but rather a roller coaster of institutional negotiation, thus metaphorically evoking the political actors' disagreements on how fundamental rights should be granted and safeguarded by the Regulation. Indeed, the resulting final version is the result of compromises between the European Commission's market-oriented vision, the Council of the EU security priorities, and the European Parliament's human-centric approach, whose intention was to impose a total ban on any type of real-time biometric identification by public or private actors without exceptions allowed.[212]

Eventually, a balance has been achieved between these three different visions. The AI Act adopts a risk-based approach, by classifying AI systems based on the level of possible threat they pose to fundamental human rights. The Regulation opens up by setting its purpose to be

> "[the improvement of] the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in

[211] A. Häuselmann, E. Fosch-Villaronga, A. M. Sears, L. Zardiashvili, *EU law and emotion data*, 2023, par. IV EU Law and Emotion Data.
[212] F. Palmiotto, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, 2024, p. 773, 782.

the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union […], including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation."[213]

This provision is significant because it frames the AI Act as a twofold instrument. On the one hand, it aims at easing the internal market through the adoption of harmonized rules. On the other hand, it stresses the utmost relevance of the protection of the fundamental rights under the Charter. Within its scope, compliance with human rights is ensured through a multi-layered system of obligations, adjusted based on the risks posed by the deployment of AI systems.

Within AI Act hierarchy, emotion recognition systems occupy a relevant position, as such they are specifically defined as

"[…] an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. It does not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents. This does also not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a

[213] European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 2024, p. 1.

smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering."[214]

This definition acquires significance as it highlights that, under the Regulation, emotion recognition is recognized as a distinct category of AI system, its main feature being the inference of emotions from biometric data. The Regulation grasps the specific risk of turning bodily or behavioral signals into evaluations about an individual's inner sphere. In addition to this, by clarifying that "physical states" and "mere detection" of readily apparent expressions fall outside the scope of the provision, unless they are used to infer emotions, the AI Act substantially differentiates between simple detection and direct inference. This distinction is legally significant as it suggests that the Regulation does not flag biometric scanning as such, but rather the inferential bridge between physiological states and psychical consciousness.

Following its risk-based structure, the AI Act identifies at its highest levels, a number of AI practices that pose unacceptable risks to the European Union values and fundamental rights and are therefore prohibited outright. These prohibitions listed in Article 5 are particularly relevant for the present analysis as it directly addresses certain uses of biometric-driven AI that may interfere with private life and personal autonomy. Among the prohibited practices one can detect

(a) "the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision […]
(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons

[214] Ivi p. 5.

(g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary […]."[215]

Notably, this provision prohibits the deployment of emotion recognition systems in the areas of education and workplace, with exceptions related to medical or safety reasons. Rather than regulating the quality or governance of AI systems, Article 5 identifies sensitive contexts in which the implementation of specific emotion recognition systems is deemed unacceptable. Particularly, by imposing a ban on emotion inference in strongly hierarchical contexts, the Regulation reflects the concern that emotion inference could actually become a tool for monitoring, evaluation and behavioral modification. From the perspective of Article 8 ECHR, these prohibitions can be read as a legislative response to the risk of disproportionate interference with private life in environments where individuals cannot meaningfully avoid, contest, or understand the inferences drawn about their emotional states.

Moving down the risk-based approach pyramid settled by the Regulation, one finds high-risk AI systems that are deemed to pose significant risks to fundamental rights, safety, and health. Their classification is listed in Article 6 in conjunction with Annex III, which provides a list of high-risk use cases. The latter identifies eight categories of AI systems that are regarded as posing a high risk to individuals. High-risk AI systems pursuant to Article 6 include systems deployed in the following areas:

[215] Ivi. p. 51, 52.

1. “Biometrics, including remote biometric identification, biometric categorization, and emotion recognition, where permitted by law, as these systems can directly affect privacy and human dignity.
2. Critical infrastructure systems where AI is used as a safety component in the management and operation of essential services.
3. Educational and vocational training systems, including AI used for student admissions, assessment of outcomes, determination of educational levels, and monitoring behavior during examinations.
4. Employment, workers’ management and access to self-employment covering AI systems used for recruitment and selection, performance monitoring, or promotion.
5. Access to essential public and private services such as systems used to assess eligibility for social benefits, or to determine risks and pricing in life and health insurance.
6. Law enforcement systems including AI used for risk assessments, evaluation of evidence reliability, detection of patterns related to criminal behavior, or assessment of the likelihood of repeat offence.
7. Migration, asylum and border control management.
8. Administration of justice and democratic processes such as AI systems assisting judicial authorities or influencing electoral behavior.”[216]

In such contexts the use of AI systems is permitted but subject to stringent requirements related to transparency, technical efficiency and human monitoring. High-risk AI systems are therefore not prohibited, but subject to strict regulatory conditions listed under Article 9-15 of the Regulation. Among them are risk management systems, high-quality data governance, technical documentation, human oversight, transparency, accuracy, robustness, and mandatory conformity assessments.

[216] Ivi p. 127,128,129.

With respect to the applications that do not fall under the scope of Article 5, such as those implemented in the commercial and retail sectors, the AI Act shifts from a prohibitive perspective to a transparency-based approach. Particularly, Article 50(3) states that

> "Deployers of an emotion recognition system or a biometric categorization system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable. […]"[217]

Under the present provision, deployers of emotion recognition systems are legally required to inform consumers in the event of being exposed to emotion detection systems. The present article aims to raise consumers' awareness regarding the collection and algorithmic interpretation of their non-verbal cues and emotional responses, thus allowing them to make informed choices, by exercising avoidance or by adjusting their behavior in response to emotion inference.

To conclude, the AI Act stands out as the first comprehensive regulatory response to emotion recognition systems in the European legal framework. Unlike earlier legal instruments such as GDPR which primarily focus on the protection of personal data, the AI Act directly addresses the inferential nature of such systems, by acknowledging the risks they pose to fundamental rights, particularly human dignity, autonomy, and the right to respect for private life.

The Regulation categorizes emotion recognition systems as tools able to turn biometric and behavioral signals into evaluative judgments about individuals' inner emotional sphere. This is the reason why the AI Act adopts a risk-based approach rather than a data-centric one. At its highest level of protection, the Regulation bans the use of such systems in workplace and educational environments. This prohibition classifies emotion inference as an unacceptable risk, incompatible with the principles enshrined in Article 8 ECHR. The Regulation further proceeds by classifying emotion recognition

[217] Ivi p. 82.

systems as highly risky when deployed in the biometric domain or in specific sensitive areas listed in the above-mentioned Annex III. Within this framework, emotion recognition is not prohibited but permitted under strict conditions only. With respect to applications falling outside the prohibited or high-risks contexts, the Regulation relies on a transparency-based approach, requiring deployers of emotion recognition systems to inform individuals when such systems are put into operation. In light of the considerations developed in this section, it can be concluded that the main objective of the AI Act is not to inhibit technological advancements, but rather to ensure that its development takes place within clear legal and ethical boundaries.

CHAPTER 3

3.1 Practical application of the AI Act within Europe: national case studies on biometric surveillance

The development toward a comprehensive European regulation related to the implementation of AI technologies cannot be fully understood without taking into consideration the jurisprudential heritage of the European Court of Human Rights. As a matter of fact, the latter has progressively reshaped the concept of interference with private life performed by private actors as well as by state and public authorities. As observed in the first chapter, the evolution of Article 8 ECHR has been marked by pivotal rulings functioning as ethical and legal foundation of the most recently promulgated AI Act.

The cornerstone case of *S. and Marper v. the United Kingdom* (2008) established the unlawfulness of indiscriminate and indefinite collection and retention of sensitive biometric data by public authorities, thus resulting in an interference with Article 8 ECHR. The judgment postulated that the implementation of such practices undermines individual dignity and autonomy by intruding into an individual's private sphere. Subsequently, the Court addressed the challenges posed by modern public monitoring technologies. In *Glukhin v. Russia* (2023), it warned against the deployment of live facial recognition technologies in public spaces for public order purposes. The Court defined such surveillance as an intrusion resulting in a chilling effect on the individual, allegedly preventing the exercise of fundamental personal freedoms. The judgments stipulated by the analyzed cases converge at a central point: the implementation of specific technological systems for law enforcement or social control requires them to be accompanied by solid procedural safeguards and meticulous impact assessments.

As extensively explored in the second chapter, modern challenges arise not only from institutional actors, but rather from the massive collection of Big Data and the deployment of algorithms and systems capable of inferring emotional states from facial detection. Concerns fostered by such fast-paced technological developments prompted the European Commission to introduce the AI Act alongside the already existing GDPR. In this context,

the EU AI Act aims at creating a comprehensive binding regulation against algorithmic control.

The present section will investigate the effectiveness of this new legal measure by taking into consideration different implementation strategies adopted by European States such as Italy, France and Spain by proposing examples of judicial decisions.[218] Particularly, the first part of this chapter will examine how national authorities are attempting to put into practice the restrictions set by the European Court, thus ensuring that AI serves as a tool at the service of the individuals rather than an opaque potential instrument of manipulation and control.

Considering this, the primary aim of the AI Act is to safeguard fundamental rights and personal data while jointly encouraging innovation and fostering trust in AI technologies. Having said that, the central core of the Regulation builds upon ethical considerations and the protection of human rights. Internal auditors should therefore assess whether AI systems are developed and implemented in a non-discriminatory way, thus fostering quality and cultural diversity.[219] As previously analyzed in the latest section of the present dissertation, the Regulation adopts a risk-based approach, categorizing AI systems into different levels of risk[220] so that obligations and requirements increase according to the level of risk the AI systems poses. Moreover, the AI Act adds a further category for models classified as General Purpose AI systems (GPAI), which are trained with a large amount of data and are able to perform several tasks.[221]

Beyond the AI systems' risk level, compliance requirements depend on the organization's specific position in the AI value chain, so that responsibilities are assigned

[218] At this point it should be clarified that, at the time of writing, no publicly available judicial decisions or enforcement actions have yet emerged that specifically address the application of the AI Act to emotion recognition systems. For this reason, the present analysis focuses on national cases concerning forms of technological surveillance and monitoring which, although not strictly involving emotional inference, anticipate the rationale and fundamental rights safeguards subsequently postulated by the European legislator. The absence of specific cases concerning the use of emotion recognition systems should not be interpreted as evidence of their legal irrelevance. It rather reflects the recently entered into force of the AI Act and the predominantly preventive function of the regulatory framework, which aims to act before the use of such systems may result in harmful effects on fundamental rights.
[219] The Institute of Internal Auditors, *The AI Act: Road to Compliance – A Practical Guide for Internal Auditors*, 2025, p. 3.
[220] They can be summarized as follows: unacceptable risk (encompassing systems that are prohibited as they violate fundamental EU values and human rights), high risk, limited risk and minimal risk.
[221] The Institute of Internal Auditors, *The AI Act: Road to Compliance – A Practical Guide for Internal*

based on the roles performed by different actors. Providers, namely the developers, have to face the most rigorous compliance standards as they place AI systems on the market, while deployers have fewer obligations, which are primarily focused on the implementation of usage protocols. With regard to providers based outside the European Union, they can rely on importers and distributors to introduce AI models on the European market. In a nutshell, the authorized representative is a person within the EU acting on behalf of the provider. Lastly, internal auditors must be aware that the role of a company may vary according to each AI system they deal with. Additionally, they must ensure that the requirements imposed by the AI Act are effectively implemented by the organizations.[222] In order to accomplish this, the Institute of Internal Auditors proposed a schedule for the AI Act's phased implementation and the corresponding deadlines for businesses. This guideline allows internal auditors to manage their organization's preparation systematically, ensuring they meet legal requirements. Starting 2 February 2025, AI literacy requirements and ban on unacceptable risk AI systems started to be applied. This includes an inventory of AI systems used by the company as well as a classification of the AI systems listed in the inventory based on the AI Act's risk categories. Moreover, deployers are required to stop using systems classified as unacceptable, while providers are obliged to remove them from the European market. From 2 August 2026, almost all provisions entailed in the AI Act will enter into force in conjunction with appropriate policies for AI systems. Lastly, by 2 August 2027, appropriate measures should be taken for the deployment of preexisting GPAI systems, while providers must ensure their products fully comply with the high-risk AI obligations.[223]

To better understand the context in which the AI Act is located, the Institute of Internal Auditors ran a questionnaire to investigate how the Regulation is applied, and the extent to which AI is used. The questionnaire was completed by more than 40 companies. The results revealed a widespread use of AI technologies, with more than half of the respondents either having already deployed AI systems or planning their implementation. The main business functions supported by standard AI and generative AI models include customer service, sales and marketing, as well as business intelligence, analytics, finance and cybersecurity. Given the fact that regulatory bodies are intensifying their demands for companies to deal with and mitigate AI-related risks, both providers and deployers have the duty to develop a

[222] Ivi p. 5.
[223] Ivi p. 8,9.

robust risk management framework. Indeed, the EU AI Act compels organizations to strengthen their existing governance structures in order to comply with new legal standards. Such regulatory alignment not only fosters safety and accountability but also enables businesses to exploit the potential of AI technologies effectively while managing the associated risks.[224]

To foster early compliance during the transitional period before the full applicability of the AI Act, in 2024 the European Commission promoted the AI Pact. The document is a non-binding recommendation which aims at encouraging organizations to align with the new regulatory requirements. In other words, the AI Pact functions as an instrument intended to support both providers and deployers in developing appropriate measures prior to the enforcement deadlines.

More in detail, the Pact is based on two pillars. Pillar I promotes collaborative engagement by inviting organizations to join a collaborative network where they can interact together with the EU AI Office to exchange experience and knowledge via interactive sessions such as workshops. Through Pillar II organizations can voluntarily commit to adopting the AI Act's key provisions before they become legally applicable. This initiative specifically encourages AI providers and deployers to proactively integrate transparency standards and compliance measures for high-risk systems.[225]

Pledges under Pillar II require organizations to comply with three core commitments with the possibility of implementing further voluntary actions to improve AI transparency, risk management and human oversight. The first point relates to strategic AI Governance and aims at encouraging organizations to develop an internal strategy in order to promote the ethical adoption of AI while aligning their operations with the upcoming requirements of the AI Act. The second core commitment entails the identification of high-risk systems. This process involves identifying and mapping any AI systems that fall into the high-risk categories defined by the AI Act. The main aim is to detect applications that could significantly affect safety, fundamental human rights or other sensitive areas of human interaction. The last point refers to AI awareness and literacy. This commitment involves

[224] Ivi p. 17,18,20.
[225] CEDPO AI and Data Working Group, *Early Compliance & Proactive Commitments: An introduction to the EU AI Pact*, 2024, p. 4.

the education of both employees and partners on how to implement AI systems responsibly. Organizations must foster a sufficient level of AI literacy among all the parties involved, enabling them to make informed decisions and recognize both the opportunities and risks associated with AI systems. In essence, these fundamental pledges establish a baseline for ethical and transparent AI operations, which is particularly relevant for companies managing high-risk models. By following this framework, the Pact provides a clear and organized method to face the ethical and societal challenges inherent in AI technologies.[226]

The AI Pact adds further optional commitments for providers of AI systems. Among the practices that they are encouraged to adopt one can mention the development of data quality policies and the implementation of concrete measures to guarantee human oversight over the operation of high-risk AI models as defined by the AI Act. Deployer guidance is jointly listed among optional commitments in order to inform deployers about how to appropriately use such technologies, their potential, limitations and possible threats. Furthermore, organizations are encouraged to outline foreseeable risks to fundamental rights of persons and groups of individuals that may be affected by the deployment of such systems.[227]

However, adherence to regulatory requirements is not limited to private actors but equally involves public institutions and authorities. As a matter of fact, the European institutional landscape is undergoing significant transformations, as European National Parliaments are progressively integrating AI systems into their operational processes. In relation to this, a survey was conducted to investigate the response of the national parliaments' administrative apparatus of the EU Member States to the fast-paced spread of artificial intelligence.

In the era of rapid technological progress, it is essential to share knowledge and practical experience regarding the regulation and use of AI.[228] Within this landscape, a survey conducted by the European Centre for Parliamentary Research and Documentation (ECPRD) investigated the EU national parliaments' response to the implementation of artificial intelligence within their administrative activities. The questionnaire consisted of

[226] Ivi p. 5.
[227] Ivi p. 6.
[228] ECPRD, *Artificial Intelligence in the Work of EU National Parliaments and the European Parliament: Survey Report*, 2024, p. 3.

eight questions and addressed to the parliaments of all EU Member States and the European Parliament. The first block of questions focused on AI regulations, specifically checking for standardization in national or internal parliamentary laws. It also aims at investigating which Parliaments or Chambers had already adopted a formal plan or strategy for AI deployment. The fourth question addressed the measures taken by Parliaments and Chambers in response to the implementation of the AI Act. Lastly, the following three questions consider whether AI tools were already in use, were under consideration or planning, or had been completely disregarded.[229] For the purpose of this thesis the focus will be on the impact of the AI Act on parliamentary administrations.

Nearly half of the respondents[230] reported both having taken concrete measures while still working on new ones following the entry into force of the AI Act. The three measures most frequently mentioned encompasses the audit of AI supported tools for officials, together with training programs for officials on the use of AI and the development of a sandbox, namely safe environment, for experimenting with AI. A smaller group of respondents reported ensuring human supervision over the use of such systems, while six respondents indicated that they had established protocols to guarantee transparency and accountability in the use of AI. All in all, the results of the survey revealed that the Irish Oireachtas and the Italian Camera dei Deputati emerged as the most active Chambers implementing measures related to the AI Act with eight different actions recorded, followed by Finland, the Netherlands and Austria.[231]

In conclusion, the survey reveals that, despite the existence of a common regulatory framework established by the AI Act, EU parliaments have reached different stages regarding the regulation and implementation of AI. Although improving efficiency in compliance with the Regulation is a shared objective, each parliament's approach is shaped by a range of factors, including different levels of so-called digital maturity, as well as the pace and scope of technological advancement. Therefore, diverse expertise, technical infrastructure, and financial resources often lead to different approaches in AI regulation and deployment across nations. The ECPRD highlights that these disparities underscore the

[229] Ivi p. 5
[230] 17 Member States representing 44,7%.
[231] ECPRD, *Artificial Intelligence in the Work of EU National Parliaments and the European Parliament: Survey Report*, 2024, p. 13, 14, 15.

need for international and interparliamentary collaboration in order to bridge existing gaps, share scientific achievements, and ultimately establish global standards.[232]

It can be summarized that there is considerable variation in AI policy maturity across European states. Countries such as France and Spain exhibit advanced levels of AI policy maturity and governance frameworks, whereas others, such as Greece and Poland, show limited policy development. This unbalanced landscape of AI policies suggests a fragmented governance environment. Although national differences reflect the specific political, economic, and institutional contexts of each Member State, they also make it difficult to create a cohesive EU governance structure. Within this context, the EU, as a collective entity, faces a watershed moment, as these disparities may hinder the implementation of the AI Act. Addressing this challenge will require stronger coordination at the EU level to support less-prepared Member States and foster greater alignment in AI governance strategies across the Union.[233]

In a still fragmented scenario, Italy gained a leading role in the implementation of the provisions under the AI Act. The Italian Act on Artificial Intelligence, approved in September 2025, represents the first piece of legislation of this kind enacted by a European Union Member State. The Italian Legislative Decree, namely *DDL IA*, aligns with the EU AI Act and entered into force on 10 October 2025. This decree is intended to support public interest objectives, including the ethical use of AI and the promotion of social inclusion through more accessible and equitable technological development.[234] As reported in Article 1, the aim of the decree is to foster the proper, transparent and responsible use of AI by adopting a human-centric perspective, in order to fully exploit the opportunities it offers. At the same time the focus is to improve the living conditions of citizens and social cohesion. In addition, the second paragraph of Article 1 expressly stipulates that all provisions must be interpreted and applied in accordance with European Union law.[235]

---

[232] Ivi p. 22.
[233] H. Costa and J. Mendonça, *Assessing European Union Member States' Implementation of the Artificial Intelligence Act*, 2024, p. 245.
[234] A. Aveni, *The New Artificial Intelligence (AI) Italian Regulation approved on 17th of September 2025: A Discussion*, 2025, p. 1, 2.
[235] Senato della Repubblica, *Disegno di Legge n. 1146: Disposizioni e deleghe al Governo in materia di intelligenza artificiale* (Provisions and delegations to the Government regarding artificial intelligence), approved on March, 2025, p. 1.

In this way, the Italian decree introduces regulatory criteria, as well as general and sector-specific rules, which promote the use of new technologies while simultaneously including measures to mitigate the risks associated with their misuse. The body of the text consists of 26 articles regulating the integration of AI across several critical sectors, which include healthcare (Article7), employment (Article 10), information management and personal data protection (Article 4), economic development (Article 5), intellectual professions (Article 12), and judicial activities (Article 14). Further provisions address user protection (Article 23), copyright regulation related to products created thanks to AI systems' assistance (Article 24), and criminal law protections (Article 25). The latter introduces an aggravating circumstance for crimes committed by using AI systems, alongside the creation of a new criminal offence related to AI misuse. Article 3 is worth mentioning as it states the core principles by requiring that the lifecycle of artificial intelligence systems and models must be based on respect for the fundamental rights and freedoms enshrined in Italian and European legislation, as well as on the principles of transparency, proportionality, security, personal data protection, confidentiality, robustness, accuracy, non-discrimination and sustainability. Development and practical application of AI systems must take place in accordance with human autonomy and decision-making power, as required by the anthropocentric approach that characterizes both the Italian decree and the European regulatory framework. Additionally, Article 3 provides that the use of artificial intelligence must not undermine the democratic life of the country or its institutions. Cybersecurity therefore must be respected throughout the entire lifecycle of artificial intelligence systems and models.[236]

Lastly, responsibility for the development of artificial intelligence systems is governed by a coordinated strategy implemented by a dedicated unit within the Prime Minister's Office, in cooperation with national authorities responsible for technological innovation, the Ministry of Enterprise and Made in Italy, and the Ministry of Universities. This institutional framework demonstrates the government's intention to maintain a central role in the development of AI systems and governance associated with them. This approach is further reinforced by the decision to assign the implementation of both national and European regulatory frameworks to the Agency for Digital Italy (AgID) and the National

[236] Presidency of the Council of Ministers, *Dipartimento per il programma di governo - Focus: Analisi del quadro normativo in materia di Intelligenza artificiale*, 2025, p. 6, 7.

Cybersecurity Agency (ACN), two technical bodies operating under the authority of the Prime Minister's Office. They play complementary roles in governing digital transformation, cybersecurity and AI systems. While AgID aims to support technological innovation, ACN is responsible for safeguarding cybersecurity and ensuring digital safety.[237]

When dealing with systems of facial end emotion recognition, it can be stated that their implementation in Italy is not widespread. Indeed, in 2021, the Capacity Decree, namely *Decreto Capienze*, primarily introduced to provide measures addressing the COVID-19 emergency, established a temporary moratorium banning the use of facial recognition technologies in public spaces and areas accessible to the public. The measure, later extended until 31 December 2025, does not however impose a complete ban. It should be noted that exceptions are allowed for activities carried out by competent authorities for the purposes of preventing and prosecuting criminal offences or enforcing criminal penalties, provided that prior approval is obtained from the Italian Data Protection Authority.[238]

However, some examples sanctioning their use can be found in the Italian legal system. A primary instance relates to the SARI[239] case. This system has been deployed by Italian State Police since 2018 in activities of investigation for crime prevention. SARI enables the comparison of images captured through surveillance cameras with those stored in a biometric database. The system can operate in both Real Time and Enterprise modes. In Enterprise mode, SARI allows operators to search for potential matches between an individual's facial image, including images obtained online, and images contained within a large pre-existing database. In order to do so, the system relies on facial recognition algorithms. Once the results produced by the algorithm have been acquired, the police officer's duty is to determine which face most closely corresponds to the individual under investigation. Human involvement, therefore, plays a central role in the identification process. Conversely, in Real Time mode, the SARI system is designed to generate immediate results from live video collected by cameras installed in public spaces. The collected data are analyzed through facial recognition algorithms and compared with

[237] M. Di Salvo, *Critical view of the introduction of artificial intelligence in the administrative procedure: Reception of the EU AI Act in Italy*, 2025, p. 11.
[238] S. Del Gatto, *Facial Recognition Through the Lens of National Legislations - Italy*, 2025, p. 70, 72.
[239] Namely, Automatic Facial Recognition System.

information contained in a watch list accessible to public authorities. Whenever a potential match is identified, the system automatically triggers an alarm.[240]

The Data Protection Authority, namely GPDP[241], intervened by classifying the instrument as unlawful, as it was used without an adequate legal basis. According to GPDP, real-time facial recognition enables large-scale automated surveillance that may involve individuals attending political or social events who are not the subject of the investigation. The Authority therefore argued that this technology fundamentally alters the nature of surveillance, shifting it from the targeted monitoring of specific individuals to potential indiscriminate mass surveillance. Considering this, the deployment of SARI real time has been prohibited.[242] In this sense, the AI Act can be regarded as a normative crystallization of principles already elaborated through judicial oversight.

The strictness imposed by the Italian regulatory approach is further exemplified by the authorities' action against private entities with overseas registered offices. A significant example of the Italian approach to biometric systems is provided by the Clearview AI case.[243] In 2022, the GPDP sanctioned the US-based company Clearview AI with an administrative fine of 20 million euros after assessing that it had carried out biometric surveillance practices affecting individuals located in Italy. Furthermore, it prohibited the further collection and processing of personal data related to Italian citizens. The company is reported to own a vast database containing more than 10 billion facial images collected globally. These images have been gathered from publicly accessible online sources, including news websites, social media platforms, and online videos, through web scraping

[240] S. Del Gatto, *Facial Recognition Through the Lens of National Legislations - Italy*, 2025, p. 73.
[241] It is an independent administrative body established by the Privacy Act (Law No 675 of 31 December 1996), subsequently regulated by the Personal Data Protection Code (Legislative Decree No 196 of 30 June 2003). The latter confirmed that the Data Protection Authority is the supervisory authority designated for the purposes of implementing the General Data Protection Regulation (EU) 2016/679 (Article 51). Garante per la protezione dei dati personali, *L'Autorità - Chi siamo* (The Authority - Who we are), available at https://www.garanteprivacy.it/home/autorita, accessed 10 May 2026.
[242] S. Del Gatto, *Facial Recognition Through the Lens of National Legislations - Italy*, 2025, p. 73.
[243] It should be specified that the Clearview AI case is not limited to the Italian legal system. Indeed, several European data protection authorities (including France, Greece and the Netherlands) have taken actions against the US company. The member states have imposed administrative fines, bans on data processing and orders to delete unlawfully collected biometric data. This series of national decisions reflect a consistency in the European approach with respect to the large-scale scraping and processing of facial images, thus confirming the incompatibility of such practices with the GDPR and anticipating the stricter prohibitions subsequently entailed in the AI Act.

techniques. More precisely, the company scraped billions of facial images from publicly accessible online sources and subsequently processed them using facial recognition technologies for identification purposes. The GPDP found that Clearview had infringed GDPR provisions, as these activities were carried out without a valid legal basis and in the absence of any transparency towards data subjects.[244]

The Italian judicial decision can be considered a precursor of the AI Act by anticipating several key issues which have been subsequently addressed by the latter, particularly the prohibition of certain biometric practices deemed incompatible with fundamental human rights. When considered in conjunction with Article 8 ECHR, this sanction carried out against Clearview shows how national authorities already aimed to limit disproportionate interference with private life before the entry into force of the European AI regulatory framework. Indeed, the final draft of the AI Act introduced the prohibition of the use of AI systems to create or expand facial recognition databases through indiscriminate scraping of facial images from the internet or from closed-circuit television footage. It furthermore prohibits the use of facial and emotion recognition systems to infer the emotions of natural persons in workplace or educational settings.[245]

Following the analysis of the Italian model, the focus will now shift to the French one. Like other Member States, France has already adopted sector-specific measures, as well as guidelines and policy initiatives. It has also begun planning for national implementation, including the designation of the competent authorities required under the EU AI Act. Nonetheless, as of September 2025, no single national AI law was enacted by French authorities. The French approach has instead favored sector-specific regulation and industry guidelines, thereby preferring a measured approach alongside the EU AI Act.[246] Within this framework the CNIL (French Data Protection Authority) plays a pivotal role in the enforcement and implementation of the AI Act in conjunction with GDPR. CNIL also acts as market surveillance authority. In order to support both private and public organizations

[244] Garante per la protezione dei dati personali, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani,* 2022, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323, accessed 10 May 2026.
[245] A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea iacta est*, 2024, p. 1120.
[246] A. Aveni, *The New Artificial Intelligence (AI) Italian Regulation approved on 17th of September 2025: A Discussion*, 2025, p. 6.

in complying with the European regulatory framework, the CNIL provides a comprehensive set of tools tailored to their specific size and needs. At the same time, the CNIL seeks to ensure that organizations can pursue their legitimate objectives while fully respecting the fundamental rights and freedoms of individuals. In this context, investigations constitute an effective enforcement mechanism targeting data controllers and processors, enabling the CNIL to verify the practical implementation and compliance with both the GDPR and the applicable legal framework.[247]

Contrary to the Italian model, the French approach to the AI Act is characterized by a gradual transition led by the CNIL. Rather than immediately adopting a standalone national AI law, the French authority has focused on providing detailed guidance on the development of AI systems in order to fully ensure compliance with the GDPR. In January 2026 the French Data Protection Authority published its first set of recommendations on the application of the GDPR to the development of artificial intelligence systems. The proposed guidelines were developed by taking into strong consideration that training datasets may entail personal data, namely information relating to identifiable natural persons. The use of such data involves potential risks for individuals that must be carefully considered in order to develop AI systems in a manner that respects fundamental rights and freedoms, including the right to privacy. It should also be specified that CNIL recommendations consider not only the GDPR, but also the AI Act. In fact, whenever personal data are used in the development of an AI system, both the GDPR and the AI Act apply. Accordingly, the CNIL's recommendations are designed to ensure a consistent interplay between these frameworks with regard to data protection.[248]

In this context, France has paid close attention to the use of automated monitoring and data analysis technologies in public places and commercial settings. Although these areas are not subject to the absolute prohibitions envisaged by the AI Act, they raise significant concerns regarding transparency and the proportionality of the interference with individuals' private lives. The Samaritaine case of 2025 falls precisely within this framework, standing out as a striking example of how the French authorities concretely applied the principles of

[247] CNIL, *The CNIL's missions*, 2025, available at https://www.cnil.fr/en/cnil/cnils-missions, accessed 10 May 2026.
[248] CNIL, *AI system development: CNIL's recommendations to comply with GDPR*, 2026, available at https://www.cnil.fr/en/ai-system-development-cnils-recommendations-to-comply-gdpr, accessed 10 May 2026.

the AI Act in conjunction with those of the GDPR, particularly with regard to systems involving the automated interception and analysis of acoustic signals, thus addressing the protection of the right to privacy in retail sector.

The case originated from the placement of new cameras capable of recording sounds carried out by the company Samaritaine SAS in its warehouses. More in detail, the cameras were disguised as smoke detectors and were capable of recording audio. Based on the findings of the investigation, the CNIL imposed a fine on Samaritaine SAS for multiple violations of the GDPR. Following the judgments of the European Court of Human Rights, the Committee emphasized that the use of covert surveillance cameras by employers may only be justified under exceptional circumstances. It further stated that such measures can be deemed lawful only when a fair balance is achieved between the legitimate aim pursued, and the employees' right to privacy. In order to comply with the principle of proportionality, the surveillance system must, for instance, be limited in duration and implemented only following a documented assessment confirming its compliance with the GDPR and the existence of exceptional circumstances. The alleged breaches attributed to the company relate in particular to the failure to comply with the obligation to process data lawfully together with breach of the principle of liability. Even though the new devices were intended to be temporary and had been installed following a series of thefts, the company failed to carry out prior assessment of the measure's compliance with the GDPR and did not formally document the temporary character of the surveillance arrangement. Moreover, employees became aware of the hidden monitoring only several weeks after the system had been installed. A further alleged breach concerns the failure to collect adequate, relevant and necessary data, as the surveillance cameras were equipped with microphones, resulting in the recording of employees' conversations, including discussions relating to their private lives. The CNIL concluded that the audio recording of employees was disproportionate and exceeded what was necessary for the stated purpose, thus violating GDPR principles.[249]

Although artificial intelligence systems were not directly involved in the case analyzed above, French enforcement practice confirms that the principles enshrined in Article 8 ECHR continue to function as a substantive benchmark for assessing the

[249] CNIL, *Hidden cameras: the CNIL sanctions the SAMARITAINE*, 2025, available at https://www.cnil.fr/en/hidden-cameras-cnil-sanctions-samaritaine accessed 11 May 2026.

lawfulness of surveillance technologies, operating alongside the AI Act and the GDPR. This demonstrates that the protection of the right to respect for private life is considered a central reference point in the assessment of technologically mediated forms of monitoring, irrespective of whether such practices fall within the material scope of the AI regulation.

The third illustrative example of the practical implementation of the AI Act within the European Union is provided by Spain. According to a survey conducted by the OECD[250] to assess the achievement of EU Member States in implementing the EU Coordinated Plan on Artificial Intelligence, Spain was the first to establish a dedicated authority for AI oversight, namely the Spanish Agency for the Supervision of Artificial Intelligence (AESIA). The agency pursues the aim to ensure compliance with applicable EU legislation and promote public awareness regarding the societal implications of AI technologies. While the Spanish Data Protection Agency (AEPD) continues to play a central role in monitoring AI-driven practices involving the processing of personal data, the newly established AESIA is responsible for supporting the effective application of the AI Act. In addition to this, Spain has also taken a pioneering role in the implementation of AI regulatory sandboxes. Such initiatives are intended to ease cooperation between regulatory authorities and companies developing AI systems, by contributing to the identification of best practices in order to support the practical implementation of the AI Act.[251]

In this regard AESIA has published sixteen guidance documents[252] intended to support compliance with the European AI Regulation. These guides were developed within the framework of Spain's pilot AI Regulatory Sandbox, an initiative aimed at facilitating both the implementation of and adherence to the AI Act. In particular, the documents provide practical and non-binding recommendations designed to assist organizations in aligning their practices with the requirements of the AI Act, pending the adoption of harmonized rules applicable throughout all EU Member States. The sixteen guides are organized into three main categories. The first one consists of introductory guides which

[250] Namely the Organisation for Economic Co-operation and Development. It is an international organization with the aim of shaping policies that foster prosperity and opportunity, underpinned by equality and well-being. It collaborates with policy makers, stakeholders and citizens to set up international standards in order to find solutions to social, economic and environmental challenges. OECD, *About the OECD*, 2026, available at https://www.oecd.org/en/about.html, accessed 11 May 2026.
[251] OECD, *Progress in Implementing the EU Coordinated Plan on AI (Vol. 1): Spain*, 2025, p. 1.
[252] AESIA, *Compliance Guides for the AI Act*, 2026, available at https://aesia.digital.gob.es/en/guides, accessed 11 May 2026.

provides a general introduction to the AI Act. These documents are intended to foster understanding of the regulatory framework through supporting materials and hypothetical use cases to illustrate the application of the rules. The second category focuses on the specific legal and technical obligations applicable to high-risk AI systems. Particularly, they address conformity assessment procedures, quality and risk management systems, data governance requirements, transparency obligations, as well as oversight mechanisms, system accuracy, robustness and cybersecurity standards. The final category consists of a guide delivering a structured methodology enabling organizations to assess their level of compliance, identify potential gaps or deficiencies, and develop a conformity plan.[253]

The Spanish model moreover reveals a national implementation trajectory characterized by a structured and anticipatory approach to AI governance. This approach is particularly reflected in the draft approved in 2025 of the national law on the Good Use and Governance of Artificial Intelligence. The latter has been specifically conceived to organize and operationalize the implementation of the requirements established under the EU AI Act at the national level.[254] The draft is conceived as a hybrid regulatory instrument that aims to balance protective regulation with the promotion of innovation. On the one hand, it establishes safeguards through prohibitions, obligations applicable to high-risk AI systems, sanctions, and market surveillance mechanisms. On the other hand, it encourages technological development and regulatory experimentation through the introduction of national regulatory sandboxes alongside practical guidance measures. The bill also requires periodic reporting by AESIA on enforcement activities, incident statistics, sandbox outcomes, and guidance publications. In addition, it mandates systematic impact assessments of enforcement practices, accompanied by periodic reviews of the list of prohibited AI practices.[255]

A relevant example of the Spanish approach is offered by the Mercadona case, which concerna the deployment of advanced surveillance technologies within retail environments

[253] E. Valín and R. Oriol, *New AESIA Guidelines to support compliance with the AI Act*, 2026, available at https://www.hsfkramer.com/notes/madrid/2026-posts/ebulletin-new-aesia-guidelines-to-support-compliance-with-the-ai-act-february-2026, accessed 11 May 2026.
[254] F. Denaro, *Artificial Intelligence Governance in Public Administration: National Regulatory Approaches in Italy and Spain under the EU AI Act*, 2025, p. 12.
[255] Regulations.ai, *Spain – AI Governance Bill, Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial, Draft Bill for the Good Use and Governance of Artificial Intelligence,* 2025, available at https://regulations.ai/regulations/RAI-ES-NA-DADLGXX-2025, accessed 11 May 2026.

open to the public. Although this case originated before the entry into force of the AI Act, it remains central to this analysis, as it illustrates the rights-based reasoning underpinning the European legislature's subsequent prohibition of certain biometric surveillance practices. The verdict delivered by the AEPD anticipated the core logic of the AI Act by subjecting facial recognition technologies deployed in publicly accessible commercial spaces to a strict scrutiny based on necessity, proportionality and the protection of private life under Article 8 ECHR.

The case originated in 2020 when the Spanish supermarket chain Mercadona S.A. introduced in several stores a system based on facial recognition technology to identify individuals subject to judicial restraining orders and prevent them from entering its premises. Cameras were installed at their entrances and captured the facial images of all customers and employees. Following a careful investigation, AEPD concluded that the facial recognition system deployed by Mercadona constituted an unlawful processing of biometric data, in breach of the GDPR and domestic data-protection law and ordered its immediate suspension.

Additionally, the Spanish authority rejected Mercadona's justification which stated that the very short retention period (approximately 0.3 seconds) excluded the existence of data processing. AEPD therefore clarified that any collection and subsequent comparison of facial images still constitute processing of personal data. The AEPD expressly rejected the classification of Mercadona's security objectives as an essential public interest, emphasizing that the applied system primarily served private commercial interests rather than a legitimate public security purpose.[256]

The AEPD postulated that, although the implemented systems might be technically effective, such effectiveness does not necessarily amount to necessity. The facial recognition system was assessed to be neither necessary nor proportionate, as it required the biometric identification of all customers and employees, including minors, in order to identify only a very small number of targeted individuals. This was deemed unjustified and

[256] Agencia Española de Protección de Datos (AEPD), *Resolución de Terminación del Procedimiento por Pago Voluntario*, Procedimiento *Nº: PS/00120/2021*, 2021, p. 52.

disproportionate in light of the existence of less intrusive means capable of achieving the same objective.[257]

In conclusion, the analysis carried out in this section shows that the AI Act does not arise in a legal vacuum, nor does it constitute a fundamental break from the existing European framework for the protection of fundamental rights. On the contrary, the national cases examined demonstrate a continuity between enforcement practices already existing before the AI Act and the risks-based approach on which it is based. The AI Act can therefore be understood as a process of legal consolidation, transforming judicial and administrative standards into a uniform preventive regulatory framework. Furthermore, the analysis shows that the current lack of complete uniformity in the implementation of the AI Act should not be understood as resistance or fragmentation. Even though Member States differ in their levels of regulatory maturity and institutional readiness, they are progressively introducing norms, policy measures, and enforcement practices aimed at aligning with the objectives of the AI Act. This ongoing process suggests that the European model of AI governance is evolving through a process of gradual harmonization in which the European Regulation acts as a reference point guiding Member States toward a common and shared objective. In this sense, differences among Member States reflect transitional phases within a shared direction, rather than divergent interpretations of the Regulation's fundamental aims.

3.2 Privacy protection in the United States: AI regulation and emotion recognition systems

The analysis carried out in the previous section has given evidence of how the European Union has developed a comprehensive regulatory framework aimed at protecting fundamental human rights and mitigating the risks associated with the deployment of AI systems and biometric surveillance. This framework has been shaped through a series of legislative initiatives, most notably the AI Act, and strengthened by proactive enforcement by Member States and national authorities. This human-centric model, as demonstrated by

[257] Ivi p. 59,60.

the analysis of cases in Italy, France and Spain, prioritizes legal safeguards to prevent potential infringements of privacy and human dignity.

In order to comprehensively comprehend the global landscape of AI governance and regulation, it is necessary to adopt a comparative perspective by shifting the focus across the Atlantic, specifically to the United States. To understand the American response to artificial intelligence and the adopted approach, however, it is necessary to first examine the distinct roots of the U.S. understanding of privacy.

Traditionally, there is a long-standing preference in the U.S. for limited government intervention in the personal life of citizens. In other words, Americans historically prioritize individual liberty and self-reliance over government assistance. For this reason, they particularly value the ideals of life, liberty and pursuit of happiness. This perspective clarifies the reason why many Americans have looked at government involvement in privacy protection with skepticism, contrary to the European Union, which have established regulatory bodies to safeguard citizens' privacy rights. In the United States privacy is protected through a fragmented legal framework consisting of common law principles, federal legislation, constitutional protections, state laws, and, in some cases, specific provisions within state constitutions. Inevitably, the American roots of the concept of privacy protection are deeply grounded in the safeguarding of individual liberty, whereas in the European Union, as already discussed in the previous chapters, it is largely grounded in the preservation of human dignity.[258]

Americans have therefore developed their unique concepts of personhood, inevitably shaped by their own historical traditions and values. As a result, certain practices are often perceived as clear violations of privacy, particularly when they involve state interference. Government action, more than private conduct, tends to provoke stronger concerns in the United States with respect to Europe. This perspective reflects a long-standing mistrust of state authority, which has historically modelled the foundation of American privacy thinking. Both legal scholarship and judicial doctrine in the United States continue to look at the state as the primary threat to individual privacy. More specifically, the American understanding of privacy can be traced back to the late eighteenth century, particularly to the Bill of Rights,

[258] A. Levin & M. J. Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2005, p. 359, 360.

which established strict limitations on governmental power. In this context, privacy is closely linked to the Fourth Amendment, which protects individuals against unlawful searches and seizures. At its core, this right reflects the idea that citizens, as autonomous individuals, possess control over their private lives and spaces, into which state intrusion is generally prohibited.[259]

This vision is inevitably reflected in the legal framework, which generally provides stronger protection against the collection and use of personal information by government institutions than by private-sector entities. The United States has traditionally been less prone to impose extensive regulatory controls on private-sector activities, by preferring to rely on market-based mechanisms and self-regulation. This approach clearly reflects the longstanding American preference for limited government intervention and its historical distrust of centralized state authority. A primary example is provided by the Privacy Act of 1974. It stands out as the only comprehensive federal legislation specifically designed to protect informational privacy. Even though its scope is limited to data processing activities carried out by the federal government and does not extend to private-sector organizations, the Act requires federal agencies to collect personal information directly from the individual. Moreover, it states that only relevant and necessary information can be retained, while records must be accurate, complete, and up to date. It also grants individuals the right to access, review, and request corrections to their records, while obligating agencies to implement appropriate safeguards to protect the security and confidentiality of the information. A further example of the American approach is the Privacy Protection Act of 1980. Despite its title, the Act primarily intends to grant freedom of speech and First Amendment rights rather than privacy in its entirety. It prohibits the government from searching or seizing materials held by citizens for the purpose of public dissemination without proper judicial authorization. Lastly, the Identity Theft and Assumption Deterrence Act enacted in 1998, criminalizes the unauthorized use of another person's identity for fraudulent or other criminal purposes. Even though the Act formally recognizes individuals whose identities have been stolen as victims, it does not directly establish preventive privacy

[259] J. Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 2004, p. 1211, 1212.

protection. It just introduces criminal penalties for privacy violations as a deterrent against identity theft.[260]

As discussed above, privacy is considered as an essential interest protected under the Fourth Amendment. Notwithstanding this, the Supreme Court of the USA has interpreted this protection in a relatively restrictive manner, limiting the scope and circumstances in which Fourth Amendment guarantees apply, particularly through the doctrine of reasonable expectation of privacy, which defines the conditions under which Fourth Amendment protections are applicable. As we move into the era of Big Data and rapid technological development, the Court has often held that technological surveillance does not necessarily qualify as a constitutional search, particularly when information is collected without physical intrusion into private property. As a result, privacy protections may not fully extend to certain forms of modern digital surveillance as "the information is gathered without trespassing on property or opening locked cabinets and doors".[261] While this approach remains influential, it has increasingly been challenged by the rise of AI-driven systems, which inevitably expose the limitations of the Fourth Amendment principles originally designed to address forms of physical intrusion.

It is interesting to observe that, as early as 2000, it was already noted that surveillance might no longer be limited to government actors, as many private-sector organizations were already engaging in extensive monitoring and data analysis. Employers, for instance, increasingly adopt tools to track employee performance and ensure productivity and integrity, while companies often analyze large datasets to identify consumer preferences and target potential customers. Even when such surveillance is not constantly exercised, the mere possibility of being observed can shape human behavior, as awareness of potential monitoring influences how individuals act.[262]

The practical implications of excluding private actors from rigid constitutional regulatory framework are widely perceived within the workplace environment. In the absence of proper constitutional safeguards applicable to private entities, the employment

[260] A. Levin & M. J. Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2005, p. 362,363,365.
[261] A. S. Khan, R. Gul, S. Naznin & Y. Khan, *The Right to Privacy, Its Progress & Decline: A Critical Review*, 2022, p. 334.
[262]A. M. Froomkin, *The Death of Privacy*, 2000, p. 1463.

sphere has increasingly become a free-for-all land for pervasive monitoring systems. While the Fourth Amendment provides a shield against state intrusion, it provides limited coverage against private actors. Within this regulatory asymmetry, employers progressively justify the deployment of invasive technologies as legitimate tools in order to grant productivity, corporate security, and operational consistency. By 2000, it had already been suggested that the workplace landscape would become a fertile ground for extensive data analysis practices, where the power imbalance between employer and employee tends to render privacy protection less effective, making it difficult to apply in everyday working practices.[263] In this context, the deployment of facial emotion recognition systems stands out as the latest and most invasive form of workplace surveillance. The integration of such AI-driven systems raises questions regarding consent, privacy and employees' wellbeing.

In the United States, workplace surveillance involves a wide range of practices. Employers exploit surveillance systems to monitor employees in order to prevent theft or fraud, assess workers' productivity for rewards or disciplinary measures and to enforce safety and workplace conduct standards so that they align with corporate value and brand standards. Workplace surveillance has become widespread, intrusive and subject to limited regulation. Indeed, in many states, employers can legally record their employees through video and audio monitoring systems, including those who work from home, by taking computer screenshots, accessing emails and by tracking workers' movements outside the workplace through company-provided devices. Recent research has shown that nearly half of employers monitor every keystroke made on company devices, while the use of passive sensing technologies in the workplace continues to expand. Although notifying employees about workplace surveillance is an important first step, the mere notification does not guarantee that workers can refuse monitoring without facing negative consequences. Moreover, many organizations justify the deployment of digital surveillance as a supporting measure, defining it as a tool for employee development, enhanced safety and workplace positivity. Similarly, the monitoring and analysis of employee's emotional states is often legitimized by affirming they can contribute to organizational competitiveness through intellectual capital, customer service, organizational reactivity, production, or the ability to attract and retain employees. Current workplace emotion-monitoring technologies are

[263] Ibidem.

marketed as essential tools for reducing absenteeism, strengthening communication and team cohesion, improving performance and creativity, supporting decision-making and negotiation, while enhancing employee health, well-being, and productivity. Notwithstanding this, many of such claims are insufficiently verified. This raises concerns for both regulators and workers as such technologies may be used not only to assess emotional states but also to monitor broader aspects of employee behavior, performance, and compliance with organizational policies.[264]

However, recent studies have highlighted that workers' perceptions of and experiences with emotion AI within the workplace environment remain underexplored. In order to address this gap, an interview study has been conducted involving 15 adult workers in the United States. Findings disclosed that participants regarded emotion AI as a deep privacy violation, particularly due to its access to sensitive emotional data. Observations suggested that such emotion systems may enforce workers' compliance with emotional labor expectations, thus leading to employees deliberate emotional regulation as means of privacy preservation. Furthermore, the study indicates that the use of emotion AI in workplace settings may expose employees to a wide range of potential harm, including privacy violations and increased pressure to conform to organizational expectations.[265]

In this regard, it is important to highlight that participants' concerns were not only how and to what degree they were monitored, but rather what was monitored, namely their emotions. They drew a clear distinction between emotions they intentionally express and those they internally feel, thus emphasizing that emotion AI's attempt to infer feelings beyond what they choose to display constitutes a significant infringement of personal boundaries. One participant described technology's capacity to detect deeper felt emotions as comparable to spying, crossing a significant privacy threshold. By blurring the edges between expressed and internal emotional states, and by bypassing workers' ability to regulate what emotional information they reveal, participants viewed emotion recognition systems as an intrusion into their inner emotional lives that digs emotional information they perceive as inherently their own. Lastly, by depriving workers of control over what is known

[264] K. L. Boyd, N. Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, 2023, p. 5.
[265] K. Roemmich, F. Schaub, N. Andalibi, *Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy*, 2023, par. Abstract.

about their internal emotional states, emotion AI- driven workplace surveillance undermines employee autonomy by coercing workers to surrender private emotional information to their employers. Beyond this immediate loss of control, such surveillance also creates the potential for future harm to employees' autonomy, as employers may use insights derived from emotional data to influence, shape, or manipulate workers' feelings in ways that align with organizational interests. This is especially concerning because it extends managerial oversight beyond observable behavior, raising serious ethical concerns about the erosion of personal agency and emotional self-determination within the workplace environment.[266]

In light of these considerations, legal and policy frameworks can serve as counterweights to limit the otherwise expansive practice of workplace surveillance. However, there are currently no comprehensive laws at the federal level that directly regulate or restrict the general surveillance of private-sector workers. For most workers, legal recourse against employer surveillance is limited to a fragmented system of state-level legislation and common law privacy torts. Although such protections exist, they fail to be sufficient to effectively prevent or remedy the privacy harm experienced by employees in the workplace. Moreover, existing legal frameworks do not adequately address emotional privacy, leaving workers particularly vulnerable to emerging forms of surveillance, such as AI-based emotion recognition systems, that intrude into deeply personal aspects of individual privacy.[267]

The critical issues that emerged by the absence of a comprehensive common legal framework on emotional and biometric recognition systems are not limited to the professional sphere. A parallel dynamic has emerged within the educational sector, where the fast virtualization of learning environments has favored the deployment of automated surveillance technologies. Just as employers exploit AI to boost productivity and promote conformity among employees, educational institutions increasingly rely, in turn, on algorithmic tools with the aim of safeguarding academic integrity, particularly through remote proctoring systems.

More in detail, the digitalization of higher education has been sped up by the availability of internet access and personal computing technologies worldwide,

[266] Ivi par. 4.1.3, 4.3.
[267] Ivi par. 5.2.

transforming how higher education institutions deliver teaching, learning, and assessment. Through the adoption of learning management systems, institutions have increasingly promoted online courses, thus enabling them to provide quality education to a wider student audience. This process accelerated significantly during the COVID-19 pandemic, which promoted the need for innovative approaches to remote assessment. In response to these challenges, higher education institutions implemented digital proctoring systems to support remote examinations. Since their introduction, the demand for and use of such systems has grown considerably. The term digital proctoring involves the use of digital tools and software designed to monitor exam-takers in order to ensure compliance with examination rules and academic integrity policies. However, the implementation of such systems inevitably raises ethical implications, privacy concerns and security risks. The monitoring and surveillance involved in online examinations can result in an infringement on students' privacy and may create feelings of discomfort and anxiety. In addition, biases embedded within monitoring algorithms may disproportionately disadvantage certain groups of students, raising concerns about fairness and equity in assessment practices. A systematic literature review has highlighted significant stakeholder concerns with respect to the protection of student data and privacy together with the risk of bias and unequal treatment.[268]

Notwithstanding the risks posed by the deployment of such monitoring systems, remote proctoring has experienced a significant growth during the last few years and is regarded by higher education institutions in the United States as an indispensable tool. Indeed, the deployment of these technologies is strongly legitimized by the need to safeguard academic transparency and authenticate students' identity in the present virtualized educational environment. From this market-oriented perspective, proctoring is not perceived as an instrument of unjustified surveillance, but rather as a tool to grant fairness and equity among students. However, the promotion of these technologies does not eliminate privacy concerns. The use of proctoring systems requires striking a fair balance between maintaining exam security and minimizing intrusiveness into students' private sphere. This approach acknowledges that the deployment of AI surveillance in education must strictly comply with data protection regulations, such as the European GDPR, and

[268] S. Han, S. Nikou, W. Y. Ayele, *Digital proctoring in higher education: a systematic literature review*, 2023, p. 266, 278.

requires the institutions to adopt transparent data handling and storage policies to inform students about how their biometric and behavioral data will be processed.[269]

In this regard, the approach adopted in the United States differs significantly from the European model. While the European Commission has opted for a preventive approach, by explicitly banning the use of emotion recognition systems in educational contexts[270] through the AI Act, the U.S. regulatory model is based on a fundamentally different logic. In the United States, in fact, no general ban on such technologies exists. On the contrary, their use is generally allowed and justified on the basis of legitimately considered objectives.

The American approach therefore tends to be more permissive and fragmented with regulation relying on guidelines and recommendations aimed at promoting the responsible use of such systems, rather than on rigid ex ante limitations. In a sensitive context of power imbalance such as that of educational environment, automated surveillance software does not simply monitor the settings where exams are held, but submits physical movements, gaze patterns and facial expressions of students to algorithmic analysis, thereby running the risk of turning the educational process into another area where improperly regulated private surveillance is permitted. This normative divergence raises concerns as to whether the U.S. framework is able to effectively safeguard individuals from intrusive forms of affective surveillance. Such normative discrepancies call for a closer examination of how the American regulatory approach has evolved in recent years in the context of AI systems.

In the absence of a comprehensive federal framework, the task of regulating advanced technological practices is primarily up to the individual states. In this fragmented landscape, California has acted as a leading force with respect to American privacy regulation. The California Privacy Rights Act (CPRA) was passed in 2020 while in 2023 it superseded its predecessor, namely the California Consumer Privacy Act (CCPA), which was considered less restrictive and required further strengthening of its potential enforcement. A

[269] E-Learning Quality Network (ELQN), *The Power of Proctoring: Enhancing Knowledge Assessment in Online Education*, 2025, available at https://elqn.org/the-power-of-proctoring-enhancing-knowledge-assessment-in-online-education/, accessed 15 May 2026.

[270] Even before the promulgation of the AI Act, the Italian GPDP imposed a sanction against the Bocconi University in 2021 for using a U.S. proctoring software (namely Respondus) during remote online exams. The GPDP ruled that the processing of student's biometric data was unlawful due to the lack of legitimate legal basis, insufficient transparency, and the disproportionate and intrusive nature of the monitoring. Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021 [9703988]*, 2021.

Compliance Guide was issued in order to encourage businesses to adjust to "one of the nation's most expansive and strict data privacy law".[271]

The CPRA structurally redefines the traditional marketing-oriented American paradigm by establishing legal guarantees for consumers regarding their personal data and introducing stricter boundaries for private-sector actors. More specifically, CPRA governs any for-profit entity that collects consumers' personal data, exercises control over the purposes and methods of its processing and engages in commercial activities within the state of California. Alongside the definition of the concept of "personal information", the Act introduces a further category, namely the "sensitive personal information". While on the one hand "personal information" relates to information that identifies, pertains to, describes, or may be reasonably linked to a specific consumer or household, on the other hand, the concept "sensitive personal information" goes deeper by encompassing account credentials, financial data, precise geolocation information, racial or ethnic origin, religious beliefs, genetic data, biometric information, and other comparable categories of sensitive information. Moreover, under the CPRA, California residents are granted the right to limit the use and disclosure of their sensitive personal information, by requiring businesses to limit data processing to what is strictly necessary to perform the services expected by the consumers.[272]

Furthermore, Section 1798.185 (a)(16) mandates the California Privacy Protection Agency to issue regulations governing consumers' rights in the age of AI systems. Under this provision, the Agency is responsible for adopting regulations governing consumers' access and opt-out rights in relation to businesses' use of automated decision-making technologies, including profiling. This provision has a twofold aim. It primarily requires businesses to provide consumers with meaningful information about the logic underlying automated decision-making processes. Secondly, it requires a clear description of the likely outcomes of the technological assessment based on the collected data.[273]

At this stage of the analysis, it is important to observe that, unlike the European Union, the CPRA does not explicitly refer to emotion recognition systems. This omission reflects a

[271] Shipman & Goodwin LLP, *California Privacy Rights Act: A Compliance Guide*, June 2021, p. 1.
[272] Ivi p. 3,10.
[273] Davis Wright Tremaine LLP, *Cal. Civ. Code § 1798.100 et seq., as amended*, 2020, p. 35.

fundamental conceptual distinction between the two regulatory approaches. Whereas the European legislator adopts a specific and explicit prohibition on affective computing in sensitive contexts, the California framework addresses such systems indirectly through the adoption of broader categories. As emotion recognition systems rely on biological data to evaluate individuals, under the CPRA they are legally regulated by the combined laws covering biometrics, automated decision-making, and profiling.

Whereas California regulates AI systems primarily through the lens of consumer data privacy, Colorado has adopted a different regulatory approach by enacting the nation's first comprehensive legislation specifically designed to govern artificial intelligence, namely the Colorado Artificial Intelligence Act (CAIA). Entered into force in early 2026, the Act shifts the regulatory focus from data ownership to the prevention of algorithmic discrimination, which is defined as any condition where the use of AI systems "result in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, ethnicity, race, religion […] or other classification protected under the laws of this state or federal law".[274]

In relation to this, the Act adopts a risk-based approach, by requiring developers of high-risk AI systems to exercise reasonable care in protecting consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from such systems. Developers are required to comply with specific obligations. These include providing deployers with a disclosure statement containing prescribed information about the high-risk system, supplying the information and documentation necessary to enable deployers to conduct an impact assessment, while publishing a publicly accessible statement summarizing the categories of high-risk systems they have developed. This statement must also explain how developers identify and manage known or foreseeable risks of algorithmic discrimination associated with the development or substantial modification of those systems.[275]

[274] Colorado Senate Bill 24-205, enacted by the General Assembly of the State of Colorado, *Concerning Consumer Protections in Interactions with Artificial Intelligence Systems*, adding Part 17 to Article 1 of Title 6 of the Colorado Revised Statutes (codified as Colo. Rev. Stat. § 6-1-1701 *et seq.*), accessible at https://leg.colorado.gov/bills/sb24-205 , accessed 16 May 2026.
[275] Colorado General Assembly, *SB24-205: Consumer Protections for Artificial Intelligence*, available at https://leg.colorado.gov/bills/sb24-205 , accessed 16 May 2026.

When dealing with high-risk classification, Section 6-1-1701(9)(a) establishes that "high-risk artificial intelligence system means any […] system that, when deployed, makes or is a substantial factor in making a consequential decision".[276] In order to understand which sectors fall under this definition, this provision has to be read in conjunction with Section 6-1-1701(3), which lists eight core domains where a choice can be deemed a consequential decision: "(a) education enrollment or an education opportunity (b) employment or an employment opportunity (c) a financial or lending service (d) an essential government service (e) health-care services (f) housing (g) insurance (h) a legal service".[277]

Conversely, Section 6-1-1701 (9)(b) introduces a series of exemptions, specifying that an AI system is not considered high risk if it merely performs narrow, routine infrastructure tasks provided that such technologies are not "intended to replace or influence a previously completed human assessment without sufficient human review". [278] The Colorado legislature thereby ensures that, while routine administrative tools fall outside the scope of the Regulation, invasive systems that play a substantial role in workplace monitoring or educational assessment are subject to the Act's stringent safety requirements.

Overall, the analysis of the California Privacy Rights Act (CPRA) and the Colorado Artificial Intelligence Act (CAIA) highlights the emergence of more structured privacy frameworks at the state level within the United States. These regulations demonstrate a growing awareness of the risks associated with the processing of personal data and the deployment of automated decision-making systems, particularly through the introduction of enhanced transparency obligations and consumer rights. Notwithstanding this, the state-level regulatory landscape remains fragmented, leaving the United States without a unified and comprehensive national framework. It is within this gap that the federal executive branch has intervened to promote a more coordinated national approach. This shift toward greater federal guidance is most clearly reflected in the initiatives introduced by the White House under the Biden Administration.

A systematic federal intervention was made necessary by the advent of the so-called "AI summer". This concept is widely recognized by scholars as being characterized by the

[276] Colorado Rev. Stat. § 6-1-1701(9)(a).
[277] Colorado Rev. Stat. § 6-1-1701(3)
[278] Colorado Rev. Stat. § 6-1-1701 (9)(B).

democratization of artificial intelligence development. Unlike earlier phases, which were typically centered on achieving a single highly specific objective, this era is defined by the possibility for both individuals and organizations to design and develop AI systems tailored to their own purposes and application fields. This transformation marks a departure from standardized, benchmark-oriented objectives toward a more distributed paradigm in which AI systems are developed to address diverse, context-specific applications. The quick proliferation of new AI services and advancements in research has forced countries to establish new regulatory frameworks, driven by the ambitious objective of identifying appropriate governance models capable of addressing the wide range of AI applications. As a result, a global race toward AI regulation has started, characterized by distinct approaches across different countries. When examining the debate through the lens of human rights and fundamental freedoms, it is evident that the large-scale deployment of AI has the potential to reshape the contemporary understanding and scope of rights protection. Fundamental rights such as the right to life, human dignity, self-determination and privacy are inevitably interconnected with technological development and are increasingly influenced by the pervasive integration of AI into everyday life.[279]

Within this context, the Biden Administration promulgated in 2022 a set of guidelines under the name of *Blueprint for an AI Bill of Rights*. This non-binding document was intended to suggest principles and best practices in the application of AI systems. More precisely, its aim is to promote the development and diffusion of AI systems in accordance with human rights and democratic values, while taking into account the risks associated with their unethical or irresponsible use. Issued by the White House Office of Science and Technology, it stands out as an initial effort to articulate a set of foundational principles intended to guide the design, deployment, and use of AI systems. More specifically, the document seeks to establish a normative framework able to ensure that technological innovation is aligned with principles of accountability, transparency, and the protection of fundamental rights.[280]

[279] V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer*, 2025, p. 50.
[280] Ivi p. 52.

Within the *Blueprint for an AI Bill of Rights* five principles have been identified in order to guide the design, use and deployment of automated systems. According to the guidelines

> "You should be protected from unsafe or ineffective systems. […] You should not face discrimination by algorithms and systems should be used and designed in an equitable way. […] You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used. […] You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you. […] You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter."[281]

It can be noted that the third principle regarding data privacy reflects some key provisions entailed in the European GDPR, particularly those concerning privacy by design, privacy by default, as well as the principles of transparency and proportionality. Similarly, the *Blueprint* highlights that consent should serve as a legitimate basis for data collection only when provided freely and meaningfully. In this regard, requests for consent should be concise, clearly expressed in plain language, and structured in a way that ensures individuals can exercise control over both the collection of their data and the specific contexts in which such data will be used. Similarities with the GDPR can be also noted within the fourth principle related to notice and explanation principles, as its main objective is to provide stakeholders with clear and accessible explanations of how data is processed within large-scale databases, while ensuring that risk assessment and mitigation measures are calibrated according to the specific context and potential impact of such processing. Lastly, one should not fail to consider the fifth principle, as it entails two fundamental elements that are significantly shaping the global debate on AI governance. The first concerns the existence of an opt-out right which, despite its formal recognition, often raises questions regarding its actual effectiveness in practice. In many cases, the complexity of automated systems and

[281] White House Office of Science and Technology Policy (OSTP), *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, 2022, p. 5, 6, 7.

the limited transparency surrounding their functioning make it difficult for individuals to exercise this right in a truly informed and meaningful way. The second point considers the preservation of human oversight in the use of AI systems. Human intervention remains essential in several sensitive domains, such as healthcare, employment, and education, where decisions generated or supported by automated systems may have severe consequences for individuals' rights, opportunities, and well-being.[282]

While the *Blueprint for an AI Bill of Rights* established an important ethical framework, its non-binding nature significantly limited its immediate regulatory effect on both public and private actors. In order to transform these foundational principles into practical operational directives, the Biden Administration strengthened its federal strategy by issuing the Executive Order 14110 on October 30, 2023. Entitled *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, the Executive Order represents a pivotal advancement in operationalizing abstract normative principles into practical rules to guarantee that AI is developed and deployed responsibly.

As a matter of fact, it stands out as one of the most comprehensive executive actions on artificial intelligence, assigning approximately 150 concrete policy actions to more than 50 federal agencies. The Executive Order seeks to strengthen privacy protections, enhance national security, and promote the global competitiveness of the United States in the field of AI. Building on the less restrictive rules set by the previous Trump Administration, it introduced more stringent regulatory requirements and safety standards. In doing so, it aimed to position the United States as an international leader in the development of AI systems that are not only innovative, but also secure, trustworthy, and aligned with ethical principles.[283]

The Order clearly states that the Administration is committed to advancing and governing the development and use of AI in accordance with eight guiding principles and strategic priorities. These principles are intended to ensure that AI innovation proceeds in a manner that is safe, secure, and aligned with broader public interests, while balancing technological progress with the protection of fundamental rights, national security, and

[282] V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer*, 2025, p. 54, 55.
[283] C. Sbailò, *Executive Order 14110 Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth*, 2024, p. 276.

democratic values. It is interesting to note how the first principle mentioned in Section 2(a) states that

> "Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers—while navigating AI's opacity and complexity."[284]

The provision emphasizes that artificial intelligence systems must be designed and deployed in a safe and secure way through standardized evaluations and effective risk mitigation mechanisms. In this respect, the Order partially converges with the approach adopted by the European AI Act, which similarly emphasizes risk assessment, ex ante controls, and the need to address high-risk applications. However, unlike the European AI Act, which expressly prohibits the application of automated emotion recognition systems within sensitive social settings, Executive Order 14110 does not explicitly refer to the concepts of emotion recognition or affective computing. Rather than imposing categorical prohibitions on individual technologies, the U.S. federal framework relies on a broader regulatory approach based on general principles, risk management obligations, and institutional oversight mechanisms. This major difference reflects a flexible and adaptive model of governance, which prioritizes guidance and coordination over binding legal constraints.

Even though the Executive Order does not impose absolute bans, it acknowledges the risks posed by phenomena such as disinformation, automated decision-making processes, and various forms of social and political manipulation enabled by advanced AI systems. The framework is consequently structured around three core objectives, each aimed at ensuring

[284] Exec. Order No. 14110 of October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, October 30, 2023, Fed. Reg. Vol 88, No. 210.

that AI development remains aligned with democratic values, social stability, and the protection of fundamental rights. The first point concerns the protection of workers from AI-driven automation to prevent further weakening of economic security for middle-class workers, who are already experiencing growing economic precarity and heightened employment instability. The second objective relates to consumers' privacy protection through the issuing of stringent privacy standards for federal agencies, requiring that the development and use of AI technologies remain compliant with existing legal frameworks, including the Privacy Act of 1974. Lastly, the third point focuses on positioning the United States at the forefront of global AI governance, while at the same time placing particular emphasis on international cooperation in the development of shared ethical standards and regulatory frameworks for artificial intelligence. Taken together, these three pillars constitute the Biden Administration's comprehensive approach to AI governance, aimed at mitigating the risks associated with artificial intelligence while simultaneously fostering its social, economic, and technological benefits.[285]

A further significant step taken by the Biden Administration was the introduction in 2024 of the *Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence*. It represents a strategic document aimed at strengthening the United States' global leadership within the domain of AI. This memorandum introduces several significant developments compared with the above-mentioned Executive Order, by placing particular emphasis on cutting-edge AI models and on the definition of more detailed strategic objectives aimed at boosting American technological advancement.[286] Whilst focusing on technological innovation, as stated in Section 2(c), the United States government recognizes that it

> "[…] must continue cultivating a stable and responsible framework […] that fosters safe, secure, and trustworthy AI development and use; manages AI risks; realizes democratic values; respects human rights, civil rights, civil liberties, and privacy; and

[285] C. Sbailò, *Executive Order 14110 Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth*, 2024, p. 281, 282.
[286] C. Sbailò, *Executive Order 14110 Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth*, 2024, p. 278.

promotes worldwide benefits from AI. It must do so in collaboration with a wide range of allies and partners. Success for the United States in the age of AI will be measured not only by the preeminence of United States technology and innovation, but also by the United States' leadership in developing effective global norms and engaging in institutions rooted in international law, human rights, civil rights, and democratic values."[287]

This viewpoint further highlights the distinctive nature of the U.S. approach to AI governance, which is characterized by a strong emphasis on strategic coordination, international leadership, and flexible regulatory instruments. When compared to the more structured and legally binding framework established by the European Union, it inevitably raises questions regarding the degree of enforceability and its effectiveness in ensuring a high level of protection of fundamental rights. These concerns regarding the American system's ability to safeguard individual rights are further reinforced and justified by the substantial regulatory shift promoted by the current Trump Administration. In fact, after returning to office, the President promptly dismantled the core elements of his predecessor's regulatory framework, by favoring deregulation, minimization of administrative burdens and the strengthening of American industrial competitiveness over stricter forms of civil rights oversight and rights-based regulatory safeguards.

More precisely, the *Initial Rescissions of Harmful Executive Orders and Actions* issued on January 20, 2025, expressly revoked the above-described Executive Order 14110. Following this, through the Executive Order *Removing Barriers to American Leadership in Artificial Intelligence* adopted on January 23, 2025, the Trump Administration took a further step by withdrawing existing AI policies and directives perceived as obstacles to American innovation in artificial intelligence, with the explicit aim of strengthening the United States' global leadership AI field. The order promotes a policy oriented toward the American AI dominance, as it is essential to promoting human flourishing, economic competitiveness, and national security. In this perspective, regulatory constraints introduced under previous

[287] White House, *National Security Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing AI to Achieve National Security Objectives; and Mitigating Risks from Adversary Use of AI*, October 24, 2024, available at https://www.presidency.ucsb.edu/documents/national-security-memorandum-advancing-the-united-states-leadership-artificial, accessed 17 May 2026.

frameworks act as potential obstacles to innovation and strategic advantage. In order to operationalize this shift, the Executive Order mandates a comprehensive review of all policies, directives, regulations, orders, and other actions adopted under Executive Order 14110 of October 30, 2023, thereby marking the start of a reassessment and potential dismantling of the regulatory measures established under Biden Executive Order 14110. Such a tabula rasa approach reflects an open attitude towards the artificial intelligence sector, based on the assumption that the development and improvement of artificial intelligence tools across various sectors should not be limited. This leads to a hands-off approach, in which market dynamics are allowed to evolve freely, without ex ante regulatory guidance or predefined regulatory constraints. In this context, neither rights-based considerations nor ethical safeguards are regarded as primary principles in the political agenda.[288]

In conclusion, the U.S. approach to AI governance emerges as a complex and evolving framework. Despite the Biden Administration's efforts to take a step forward toward the articulation of common principles and the operationalization of risk-based safeguards, the absence of a comprehensive and binding federal regulatory framework continues to limit the enforceability of such measures. The subsequent political changes under the current Trump Administration further highlight the fragility of the American approach, by revealing the instability of a system relying mainly on executive decisions and political priorities. This evolving landscape underscores a fundamental difference compared to the European model, which, through the AI Act, seeks to establish a stable, harmonized, and legally binding system of regulation.

3.3 Privacy protection and AI regulation in China

Based on the analysis developed in the previous sections, it has emerged that the concept of privacy and its regulation in the era of artificial intelligence are deeply influenced not only by national legal systems, but also by underlying cultural values and ideals. Notably, section 3.1 highlighted how the European Union has developed a strongly rights-based regulatory model, grounded in the protection of human dignity and fundamental human rights. This approach, which has been consolidated through the case law of the European

[288] V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer*, 2025, p. 62,63.

Court of Human Rights and crystallized in the recently adopted AI Act, is characterized by a preventive approach and a clearly structured regulatory framework aimed at limiting the risks arising from the use of biometric AI-driven systems, paying particular attention to interference in individuals' private life.

In contrast, as discussed in section 3.2, the U.S. model is characterized by a more fragmented and market-oriented approach, in which privacy protection has historically been associated with shielding individuals from government interference rather than regulating the conduct of private actors. As a result, the American model is marked by sector-specific regulatory measures and less restrictive regulatory control over the use of AI technologies, including emotion recognition systems, whose deployment is generally permitted. A preliminary comparison of these two models thus reveals a significant divergence. While the European Union favors proactive regulation strongly anchored in fundamental human rights, the United States adopts a more flexible approach, in which privacy protection is safeguarded in a less systematic way.

Building on these considerations it is important to broaden the analysis to include the Chinese context, as it operates outside traditional Western frameworks. In China, the regulation of artificial intelligence and the protection of privacy are shaped by a profoundly different political and cultural heritage, where the balance between individual interests, state control, and collective aims assumes distinctive characteristics. To properly understand the Chinese model, it is therefore necessary to first inquire into the meaning of the concept of privacy in Chinese culture as an essential starting point for subsequent analysis of the evolution of the regulatory framework and the ways in which artificial intelligence is regulated within the country.

To comprehensively understand the cultural phenomenon underlying the evolution of the concept of privacy, it is relevant to take into account the concept of *face*, namely 面子 *miànzi*, which emphasizes the protection of personal dignity, social reputation and respect within the broader community. In Chinese culture, privacy is not primarily assessed as an individual right in the Western liberal meaning, but rather as a means of preserving social harmony by allowing individuals to determine how they present themselves to others. This cultural framework, rooted in Confucian tradition, values collective interests above

individual autonomy and regards personal conduct as deeply intertwined with family and community reputation.[289]

Unlike the relatively recently emerged Western conception of privacy, which originated from legal and moral traditions centered on individual rights and protection from state intrusion, Chinese legal thought developed within a Confucian moral philosophy that prioritized order, hierarchy and social stability. Even though Confucianism acknowledged the existence of certain forms of privacy, their purpose was not to safeguard individual autonomy. Privacy protection was rather an aftereffect of broader ethical principles intended to maintain social order. Within this vision, individuals are subordinated to the family, the community and above all the state. The traditional Chinese term for privacy, 隐私 *yǐn sī,* reflects this cultural point of view. It is associated with hidden or potentially shameful matters that individuals intend to shelter from public exposure to avoid humiliation and loss of face. As reputation extends to the family as a whole, privacy violations tend to be understood in terms of their impact on collective honor rather than personal harm. Paradoxically, in a shame-based culture, wrongdoers' public exposure has historically been used as a mechanism of social regulation. In Chinese society, the disclosure of personal misconduct is considered legitimate in order to strengthen moral behavior through collective judgment and public accountability. The influence of collectivist values was further reinforced during the Communist period, when collective living and state control left little room for private personal space or information privacy.[290]

Notwithstanding this, the subsequent economic developments, modernization processes and Western legal influences have inevitably affected this historical and cultural heritage, leading China to expand its privacy protection principles. Ultimately, it can be argued that Chinese privacy is the result of a complex interaction between Confucian ethics, communist collectivism, and Western legal influence, thus shaping a distinct understanding of privacy that differs significantly from Western individualistic approaches.[291]

This distinctive understanding is reflected in the Chinese Constitution adopted in 1982, which provides limited constitutional foundations for privacy-related protections. Notably,

[289] T. Li, J. Bronfman, and Z. Zhou, *Saving Face: Unfolding the Screen of Chinese Privacy Law*, 2018, p. 1, 2, 3, 4.
[290] Ivi p. 5, 10, 11.
[291] Ivi p. 11.

Article 33 establishes that the state respects and protects human rights. Additional guarantees can be found in Article 38, which protects citizens' personal dignity, together with Article 35, which safeguards fundamental freedoms such as freedom of speech, press, assembly, association, procession, and demonstration. The Constitution also recognizes the confidentiality and privacy of correspondence. However, despite these provisions, it does not explicitly establish a broad and general right to privacy, nor does it provide clear constitutional protection for personal data or data protection rights. As a result, privacy and data protection in China have largely developed through statutory legislation and regulatory frameworks rather than through direct constitutional recognition.[292] Moreover, following a civil law jurisdiction, China cannot develop constitutional rights to privacy and data protection just as case-law systems do. Furthermore, given the absence of a constitutional court in China, the Constitution is generally considered non-justiciable. In practice, this implies that Chinese courts are not empowered to invalidate a law or a regulation based on unconstitutionality. Consequently, the development of privacy and data protection rights in China relies on legislative and administrative actions rather than on constitutional principles or judicial interpretation.[293]

Given the limited constitutional recognition of privacy rights, the AI regulation in China must be understood through the lens of statutory policies and initiatives. More precisely, the current Chinese regulatory framework must be observed in light of China's broader national strategy to achieve global leadership in technological innovation. Since 2013, China has published a series of national policy documents which show a clear

[292] While the above-mentioned provisions of the Chinese Constitution may contribute to the protection of privacy-related interests, such protection is not articulated as a distinct and coherent fundamental right. This poses a significant difference with respect to Article 8 ECHR, which recognizes an autonomous right to private life, by imposing both positive and negative obligations on States to ensure its effective protection. By contrast, the Chinese constitutional system does not impose similar duties, as privacy-related interests are protected only indirectly through fragmented provisions. More in detail, Article 33 of the Chinese Constitution clearly states: "The State respects and preserves human rights. Every citizen enjoys the rights prescribed by the Constitution and other laws and at the same time must perform the duties prescribed by the Constitution and other laws." *Constitution of the People's Republic of China* (1982, as amended in 2018), English translation by Changhao Wei and Taige Hu, English translation by Changhao Wei and Taige Hu, NPC Observer, 2018.
The Chinese Constitution thus explicitly links the recognition of human rights to the fulfilment of citizens' duties towards the State and society, emphasizing the individual's obligations towards the State. This vision significantly differs from that of Article 8(2) ECHR, which, by stating that there shall be no interference by public authority with the exercise of the right to private life, recognizes privacy primarily as a limit on State interference and power.

[293] Y. Zhang, *Personal Data Protection and Data Transfer Regulation in China*, 2024, p. 5, 6.

intention to advance in the development and application of AI across multiple sectors. This strategic plan became evident in 2015, when the State Council promulgated guidelines on China's Internet + action with the intention of integrating digital technologies into all economic and social areas. The policy highlighted the importance of fostering AI industries and increasing investment in research and development. In the same year, the government promulgated the ten-year Made in China 2025 plan, with the aim to strengthen China's position as a global leader in high-tech manufacturing, including AI-related industries. This willingness was further reinforced in 2016 through the Chinese Communist Party's 13th Five-Year Plan, which identified artificial intelligence as one of the key strategic sectors for industrial development and as a driving force for future economic growth. Taken together, these policy initiatives demonstrate that Chinese interest in AI did not originate as a reaction to external developments, but rather as the result of a long-term and carefully planned national strategy.[294]

However, before 2016, AI was simply presented as one technology among many others, which could be useful in achieving a range of policy goals. This approach changed significantly with the publication of the New Generation Artificial Intelligence Development Plan (AIDP) in July 2017 by the State Council. The AIDP stands out as the first comprehensive and unified framework dedicated specifically to AI, thus marking a turning point in China's technological strategy. The plan sets out an ambitious long-term objective, namely

> "We shall conscientiously implement the decision-making arrangements […] and the in-depth innovation-driven development strategy to accelerate the integration of artificial intelligence and economy, society and defense and enhance a new generation of artificial intelligence scientific and technological innovation capacity as the main direction. We shall develop intelligent economy, construct intelligent society, safeguard national security, build the ecosystem with cluster integration of knowledge, technology, industry, […] foresee the risks and challenges, […] and as a result comprehensively enhance the social productive forces, national strength and national

[294] H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*, 2020, p. 60.

competitiveness for the purpose to speed up the construction of innovative countries and the science and technology power of the world, to achieve "two hundred years" goals and to provide strong support for the great rejuvenation of the nation."[295]

China has therefore set itself the goal to become the global leader in the field of AI innovation by 2030 and to put AI in the spotlight as the primary driver of industrial modernization and economic transformation. Beyond its economic objectives, the AIDP also emphasizes the strategic application of AI across a wide range of sectors, including national defense and social welfare, while highlighting the importance of developing regulatory standards and ethical frameworks to govern its use. In a nutshell, the Plan outlines a far-reaching national strategy that signals China's intention to compete with other major global powers in shaping the future of artificial intelligence.[296]

In addition to this it is worth mentioning that, with regard to the private sector, China has adopted a targeted strategy by appointing selected companies as AI national champions. The latter are officially endorsed by the government to focus on developing specific sectors of AI. For instance, Baidu has been tasked with developing autonomous driving technologies, Alibaba with smart city innovation, and Tencent with computer vision applications for medical diagnosis. This state recognition mirrors a collaborative approach in which private companies align their research and development efforts with the state's strategic objectives. In return, the so-called national champions benefit from significant institutional advantages, including priority access to public contracts, improved financing opportunities, as well as regulatory conditions safeguarding their market position. This model clearly illustrates the close integration between state planning and private-sector innovation within China's AI development strategy.[297]

Given the historical and cultural considerations outlined at the beginning of this section, it is essential to emphasize that this deep interconnection between state planning and economic/technological advancement extends beyond mere industrial or economic

[295] State Council of the People's Republic of China, *New Generation of Artificial Intelligence Development Plan*, State Council Document No. 35, 2017, p. 4.
[296] H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*, 2020, p. 60.
[297] Ivi p. 61.

improvement. It rather pursues a clearly defined social and political agenda relevant to public governance. Indeed, the Chinese paradigm of social governance extends far beyond the management of material resources and environmental infrastructures, by directly encompassing the regulation of citizens' behavior. Scholars have argued that the disruption of the Maoist era provoked profound ideological disruptions, further reinforced by the rapid economic liberalization of the following reform period. It is undeniable that such deep changes generated a perceived moral vacuum within contemporary Chinese society. As a consequence, political leaders, including Xi Jinping, have acknowledged this issue and promoted the idea of establishing a minimum moral standard within society. In this context, governance is not only perceived as the effective administration of public affairs, but also as a moral guide with the responsibility to lead citizens toward the preservation of moral integrity by supporting and promoting social morality. This peculiar understanding of governance duties aligns with the government's view that technological innovation, particularly AI, can serve as a tool for promoting social order and moral regulation. Reflecting this perspective, the New Generation Artificial Intelligence Development Plan enhances AI potential for analyzing collective cognition and social psychology, thereby supporting the state's efforts to shape behavior and reinforce societal norms. To serve this purpose, in 2014 a Social Credit System was established with the aim to regulate not only financial and corporate actions of business and citizens, but also individuals' social behavior.[298]

It was within this articulated institutional environment, shaped by swift technological expansion, government-supported national champions, and the increasing deployment of technology as an instrument of social governance, that China's comprehensive data privacy framework gradually crystallized, ultimately leading to the adoption of the Personal Information Protection Law (PIPL) in 2021. As digital technologies became an integral part of everyday life and the platform economy soared, public concerns in China regarding the misuse of personal information and insufficient data protection intensified. In light of this, PIPL represents a milestone in the evolution of global data protection regulation, frequently compared to the European Union's General Data Protection Regulation (GDPR), as it reflects similar foundational principles, including rights of access, correction, and deletion

[298] Ivi p. 66, 67.

of personal data, as well as principles of data minimization and accountability. At the same time, PIPL establishes a number of distinctive regulatory obligations. Among its key distinctions are its broad extraterritorial application and its rigorous requirements governing cross-border data transfers. In particular, the law imposes data localization obligations for entities handling large quantities of personal information.[299]

Under PIPL provisions, Article 4 promptly defines the concept of personal information by stating that it "refers to various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously."[300] The following provisions, namely Article 5 and 6 establish that personal information must be processed in accordance with the principles of legality, legitimacy, necessity, and good faith, while prohibiting practices involving deception, fraud, and coercion. Furthermore, Article 6 stipulates that the processing of personal information must pursue a clear and reasonable purpose and be carried out in a way that minimizes negative effects on individuals' rights and interests. Article 28 introduces the concept of sensitive personal information as a data category that

> "can easily lead to the infringement of the personal dignity of natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts […]. Personal information processors can process sensitive personal information only when they have a specific purpose and sufficient necessity, and take strict protective measures."[301]

The regulatory framework of the PIPL naturally lends itself to a comparison with the European GDPR. Several aspects of the PIPL's conceptual structure and underlying principles closely mirror those of its European counterpart. For example, the distinction

[299] Y. C. Zhang, *China's Personal Information Protection Law (PIPL) 2021: An Analysis*, 2021, par. Introduction, Why PIPL Was Introduced.
[300] National People's Congress of the People's Republic of China, *Personal Information Protection Law of the People's Republic of China*, Chairman's Order No. 91, adopted August 20, 2021, effective November 1, 2021.
[301] Ibidem.

drawn between general personal data under Article 4 and sensitive personal data under Article 28 mirrors the classification framework set out in Articles 4 and 9 of the GDPR. Similarly, the processing principles set out in Articles 5 and 6 of the PIPL, in particular those relating to lawfulness, necessity and purpose limitation, reflect the fundamental data protection principles enshrined in Article 5 of the GDPR.

Despite evident structural and terminological similarities, PIPL and the GDPR differ in their underlying ideological and political foundations. As already mentioned in the first part of this section, the GDPR is grounded in the Western liberal tradition of fundamental rights, where data protection is primarily conceived as a means of safeguarding individual autonomy and human dignity against unauthorized interference by both private actors and the state. In contrast, the PIPL is shaped by the institutional and ideological context of China's socialist market economy and collectivist governance model. Consequently, its regulatory focus is shifted from limiting state power to tackling the growing influence of big private tech companies. PIPL was also introduced in order to fight anti-competitive practices, algorithmic discrimination and the misuse of personal data by commercial platforms, while strengthening consumer trust and preserving social stability in a wider sense.[302]

Conversely, under European law, the protection of personal data is recognized as a fundamental right, enshrined in Article 8 ECHR. From this perspective, GDPR establishes a system in which personal data cannot be regarded as mere economic assets or objects of exchange but must be protected as closely linked to the dignity and freedom of the individual. In this light, personal data cannot be classified as a mere tradable good, but rather as an essential dimension of individual rights. As discussed in the first chapter, this approach is particularly evident in Article 9 of the GDPR, which regulates the special categories of personal data. This provision introduces a general prohibition on the processing of sensitive data, such as data relating to health, religious beliefs or political opinions, unless specific mandatory exceptions apply. The European legislator, therefore, adopts a strongly rights-based approach, in which certain data are considered inherently more dangerous to fundamental rights and freedoms and, for that reason, are subject to reinforced ex ante protection.

[302] Y. C. Zhang, *China's Personal Information Protection Law (PIPL) 2021: An Analysis*, 2021.

At first glance, the Personal Information Protection Law (PIPL) shows some similarities, though it reveals a different underlying rationale. Article 4 of the PIPL defines personal information as any information relating to identified or identifiable natural persons, excluding only anonymized data. This definition is broadly neutral and, unlike the GDPR, does not introduce a distinction between categories of data at the definition level. A distinction is made, however, in Article 28 of the PIPL, which introduces the category of sensitive personal information, defined as information which, if disclosed or used unlawfully, may easily result in an infringement of personal dignity or harm to personal or financial security. However, unlike Article 9 of the GDPR, this provision does not constitute a general processing prohibition. Rather, the PIPL imposes stricter conditions, such as the specific necessity of the processing and the explicit consent of the data subject.

This reflects a profound difference. While the European model regards personal data primarily as an extension of an individual's fundamental rights, and therefore as assets not subject to full commercial exploitation, the Chinese model places data protection within a broader framework of risk management and governance, in which the protection of the individual is balanced against public order, economic development and national security. From this perspective, even sensitive data is not subject to absolute prohibition, but to more stringent regulation, aimed at monitoring its use rather than restricting it in absolute terms.

Further differences between the GDPR and the PIPL emerge when analyzing additional provisions of the Chinese regulation, namely Articles 10, 26 and 35. Read together, these provisions reveal a regulatory approach in which data protection does not function as a constraint on state power, but rather operates as part of a broader strategy aimed at ensuring public order, social stability, and the effective exercise of state authority.

Specifically, Article 10 shows how, under the Chinese system, the protection of personal data is situated within a framework that explicitly integrates national security and public order objectives. This provision prohibits the unlawful processing of personal data not only when it infringes individual rights, but also when it endangers national security or the public interest.[303] This article reveals a significant difference. Whereas in the GDPR the

[303] National People's Congress of the People's Republic of China, *Personal Information Protection Law of the People's Republic of China*, Chairman's Order No. 91, adopted August 20, 2021, effective November 1, 2021.

restriction is based on the protection of the individual, in the PIPL it is jointly determined by collective and state interests.

Article 26 is particularly significant, as it governs the use of identification and data collection systems in public spaces, permitting such use for public security purposes. This provision is particularly relevant when considered in relation to widespread surveillance systems, highlighting how the PIPL not only does not exclude such practices, but integrates them within a regulatory framework that legitimizes their use for the purpose of maintaining social order.[304]

Finally, Article 35 of the PIPL introduces significant exceptions to the obligations of transparency towards the data subject, providing that state authorities may exempt themselves from the obligation to provide information and the requirement for consent in two main cases. The first exception occurs when the processing of data is subject to statutory confidentiality obligations. The second one, when the disclosure to the data subject would compromise the performance of institutional functions, such as investigative activities or operations relating to national security. This provision highlights how, under the PIPL framework, the protection of the individual may be limited in the presence of pressing needs linked to the exercise of public authority. Unlike the European model, in which rights' restrictions must be strictly limited and subject to a rigorous proportionality test, the PIPL contemplates broader exceptions especially when dealing with activities carried out by the state.[305]

The underlying tension within the PIPL between data protection, market regulation and the protection of state authority is deeply rooted in the structure of the law and has inevitably shaped China's regulatory landscape. This tension has laid the foundations for a new generation of sector-specific and technology-focused regulations introduced between 2024 and 2025. As China's technological landscape has advanced beyond general data protection principles towards the widespread adoption of generative artificial intelligence and advanced biometric technologies, the Chinese authorities have transformed the general provisions entailed in the PIPL into more detailed regulatory mechanisms and operational standards.

[304] Ibidem.
[305] Ibidem.

The current regulatory phase follows a mixed approach. On the one hand, the State aims to establish standardized technical measures across the technology supply chain in order to ensure regulatory consistency, industrial coordination and market stability in relation to the AI industry. On the other hand, it has introduced stringent limitations on the commercial use of high-risk AI technologies, whilst maintaining broad operational powers for public authorities in the name of public safety and social order. In order to understand the evolving Chinese framework two key regulatory developments must be considered.

A meaningful example of the state-driven market-oriented dimension of China's regulatory strategy is provided by the *Guidelines for the Construction of a Comprehensive Standardization System for the National Artificial Intelligence Industry* (2024). This document outlines a strategic framework for the creation of a unified national system of standards governing the AI industry. The Guidelines place particular emphasis on the development of technical standards related to data quality, algorithmic transparency, and model evaluation, validation and verification. Rather than focusing on limiting the development of artificial intelligence, the framework seeks to enhance research and development, promote industrial modernization, and ensure that private-sector AI products operate in accordance with State requirements, with the aim of

> "[…] standardize safety and security requirements throughout the lifecycle of AI technology, products, systems, applications, and services. They include standards for basic safety and security, data, algorithm, and model safety and security, network technology and system security, safety and security management and services, safety and security testing and evaluation, safety labeling, content identifiers, and product and application safety and security. […] Considering the actual needs of AI governance, these standards standardize the requirements for AI […] including technical requirements and evaluation methods for the robustness, reliability, and traceability of AI, AI governance support technology, and ethical governance requirements for the total AI life cycle. They include standards for AI ethical risk

assessment, AI fairness, explainability, and other ethical governance technical requirements and evaluation methods, and AI ethical review."[306]

Conversely, the security and surveillance dimensions of the Chinese regulatory framework are directly addressed in the *Measures for the Security Management of Facial Recognition Technology Applications* (2025), issued under Order No. 19 by the Cyberspace Administration of China (CAC) together with the Ministry of Public Security. As clearly stated by Article 1 and 2, these measures

"are formulated to regulate the use of facial recognition technology for processing facial information and to protect personal information rights and interests […]. These Measures apply to activities using facial recognition technology to process facial information within the People's Republic of China (PRC). […] These Measures do not apply to the use of facial recognition technology to process facial information for research and development or algorithm training purposes within the PRC."[307]

Moreover, under Order No. 19 private companies and commercial operators are subject to stringent compliance obligations. The use of facial recognition technologies in public or commercial settings requires explicit and separate consent from individuals, must satisfy strict standards of specific necessity, as well as provide alternative non-biometric methods of access or verification. In this regard, Articles 11, 12 and 13 are of particular relevance as they clearly postulate that

"[…] When using facial recognition technology to verify personal identity or identify specific individuals, it is encouraged to prioritize the use of channels such as the

[306] Ministry of Industry and Information Technology, Office of the Central Cyberspace Affairs Commission, National Development and Reform Commission, and Standardization Administration of China, *Guidelines for the Construction of a Comprehensive Standardization System for the National Artificial Intelligence Industry (2024 Edition),* issued June 5, 2024, p. 12, 13.
[307] Cyberspace Administration of China and Ministry of Public Security, *Measures for the Security Management of Facial Recognition Technology Applications*, issued March 13, 2025.

National Population Basic Information Database […] and National Network Identity Authentication Public Services […] in order to reduce the collection and storage of facial information and safeguard its security. […]

No organization or individual shall mislead, defraud, or coerce individuals into accepting identity verification via facial recognition technology on the grounds of business processing or improving service quality. […] The installation of facial recognition equipment in public spaces must be necessary to maintain public security. The facial information collection area shall be lawfully and reasonably defined, and clear signage must be displayed.

No organization or individual shall install facial recognition equipment inside private areas of public places, such as hotel guest rooms, public baths, public changing rooms, or public restrooms."[308]

Upon reading these provisions it is immediately noticeable that they align with the regulatory logic reflected in Articles 26 and 35 of the PIPL, as they preserve the surveillance powers of the state. Public security authorities and law enforcement agencies are exempt from the restrictions imposed on private commercial actors when facial recognition technologies are used for purposes related to national security, crime prevention, or the maintenance of public order. As a result, these regulatory measures do not fundamentally restrict China's algorithmic governance system. Instead, they establish a differentiated regulatory structure within the deployment of biometric surveillance technologies. While the commercial use of facial recognition systems by private companies is subject to strict oversight, prohibitions and regulation, the same category of systems employed for state governance is simultaneously legitimized and institutionally embedded.

It can be summarized that China's legal and regulatory framework has gradually evolved from a system based on broad general principles toward a model of more specialized governance in response to emerging technological challenges. Before the adoption of the PIPL, the Civil Code and the Cybersecurity Law did not distinguish

[308] Cyberspace Administration of China and Ministry of Public Security, *Measures for the Security Management of Facial Recognition Technology Applications*, issued March 13, 2025.

biometric information from ordinary personal data, resulting in a uniform level of protection that failed to encompass the higher risks associated with sensitive biometric technologies. The introduction of the PIPL, together with subsequent implementing measures, marked an important step toward a specialized regulatory framework by explicitly categorizing facial recognition data as sensitive personal information and introducing safeguards such as separate consent requirements and the obligation to provide non-biometric alternatives for identity verification. Despite these developments, significant regulatory gaps remain in translating broad legal principles into concrete operational standards. In particular, there is still no authoritative and unified interpretation clarifying how separate consent should be obtained in public settings where data collection often occurs without meaningful user interaction, nor are there precise criteria defining the threshold of minimum necessity. As a result, substantial uncertainty persists both for companies attempting to comply with the law and for regulators responsible for its enforcement.[309]

The differentiated regulatory structure identified above becomes particularly evident when examining the role of AI in law enforcement and state surveillance practices. In confirmation of the above-discussed points, Article 19, an international human rights organization, in a 2021 report investigates the rapid expansion of emotion recognition technologies in China. The main purpose was to evaluate their harmful implications for individual liberties and human rights. The report highlights how these technologies are becoming increasingly embedded in key areas of daily life. For instance, law enforcement agencies employ them to identify individuals considered suspicious, while educational institutions use them to monitor students' attention levels in classrooms. With respect to law enforcement, Chinese law enforcement agencies and public security bureaux have shown growing interest in emotion recognition software as a tool for interrogation and criminal investigation. Several companies actively pursue procurement order contracts for state surveillance projects and provide training programs for police officers on the use of their technologies. In some cases, firms market their products to law enforcement authorities by

[309] L. Jiang, *The Current Situation and Risk Prevention of Facial Recognition Technology in China: A Legal and Governance Perspective*, 2025, p. 61.

suggesting that these systems could potentially circumvent certain procedural safeguards, including those related to self-incrimination.[310]

A research paper produced by scholars at the Hubei Police Academy points out how facial micro expressions can be exploited in order to identify individuals considered dangerous or high-risk groups, even when they have no previous criminal history. The study suggests developing databases containing video footage of offenders both before and after crimes are committed in order to train algorithms to recognize facial movements and behavioral patterns. The assumption underpinning the applications of emotion recognition systems in public security is that individuals experience feelings of guilt prior to committing crimes. The concealed emotional states inevitably manifest through subtle, involuntary facial expressions that can be detected by high-resolution surveillance technologies. In addition, several emotion recognition companies claim that their technologies are capable of identifying sensitive personal features, including mental health conditions and racial identity. However, these companies rarely address the potentially discriminatory implications of collecting and processing such data alongside emotional information. Some application programming interfaces contain problematic racial classification categories. Furthermore, companies asserting that they can diagnose neurological or psychological disorders through facial emotion analysis often fail to explain how these assumptions may affect the use of emotion recognition systems in non-medical contexts, such as schools or workplaces, where inaccurate or biased interpretations could lead to harmful consequences.[311]

Notwithstanding the several critical issues posed by these artificial intelligence-based systems, which have been already discussed in the second chapter, the People's Republic of China has developed the world's largest public surveillance system based on artificial intelligence, relying increasingly on AI systems to perform many of the tasks that were once carried out by human police officers. Just like drone operators, police personnel in Chinese cities now often work from command centers, where they monitor and manage public safety via screens displaying data collected, processed, filtered and visualized by artificial intelligence systems. As a result, AI is increasingly capable of managing the entire law-

[310] ARTICLE 19, *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, 2021, p. 5, 6, 7.
[311] Ivi, p. 19.

enforcement process, including information gathering, command operations, planning, and patrol activities. Technological advancements have enabled massive data integration not only across urban areas but also throughout the country, including rural regions. The Chinese Communist Party is setting up a national digital command center. As the current surveillance system in China is often criticized as onerous, inefficient, and heavily dependent on human labor, the CCP aims to develop a more automated surveillance infrastructure that relies on artificial intelligence rather than human involvement. A further advantage that PRC authorities hope to gain from AI is the possibility to answer citizens' questions and complaints before dissatisfaction escalates into frustration, anger, or unpredictable behavior. Therefore, AI systems equipped with reasoning capabilities are being incorporated into municipal services.[312]

The implications of such an extensive and increasingly automated surveillance infrastructure became particularly evident in specific regional contexts, leading to severe negative consequences and to violation of human rights. A clear example of this can be found in Xinjiang region, where the Chinese government has implemented these technologies to counteract religious extremism by monitoring the Uyghurs, a Muslim ethnic minority. The aim pursued by the Chinese government is the Uyghurs digital and physical monitoring, thus leading to severe consequences for individuals' daily lives. As part of the extensive surveillance system deployed in the People's Republic of China, the daily lives and online activities of the Uyghur population are subject to extensive monitoring. This surveillance encompasses nearly all forms of digital activity, including social media posts, private messages, and web browsing. It is reported that online monitoring has also enabled coercive practices, such as interrogations and pressure on Uyghurs to monitor or report on one another. In addition to online monitoring, Uyghurs experience pervasive physical surveillance in everyday life. This includes widespread use of surveillance cameras, facial recognition systems, police inspections, and ID-scanning devices. Security cameras are installed at the entrances of residential buildings, mosques, schools, streets, and public spaces such as airports, train and gas stations. Although the exact number of cameras

[312] V. Weber, *China's AI-Powered Surveillance State*, 2025, p. 151, 153.

equipped with biometric capabilities remain unclear, facial recognition technologies are known to be deployed throughout the whole region.[313]

Such systematic surveillance and repressive practices resulted in significant psychological, behavioral, and social side-effects for the Uyghur population. Interviewees reported experiencing feelings of fear and anxiety even while living or traveling abroad, as they continue to feel constantly monitored. In reaction to this, many Uyghurs adopt precautionary measures and engage in self-censorship to avoid attracting attention from authorities. Communication with others, including local communities, is often limited because of fears that interactions may place them or their relatives at risk. They also expressed concern that the increasing use of advanced technologies could contribute to the emergence of a dystopian society characterized by pervasive state surveillance.[314]

This trend toward an increasingly automated and pervasive surveillance architecture has also been interpreted through the concept of the "sentinel state", which describes a political system in which advanced monitoring technologies play a fundamental role in ensuring the survival of authoritarian rule. In this context, it has been argued that the dystopian world described in 1984 by George Orwell, once regarded as pure science fiction, appears to be turning into reality when considering the Chinese government's aggressive adoption of the world's most advanced technologies. Supporting evidence of this is the fact that the ruling Chinese Communist Party appears to be eager to expand its already extensive surveillance powers. Among its initiatives is the already mentioned social credit system project, which would enable the authorities to assess individuals' political loyalty and to predict their future behavior based on data derived from their social and economic activities. This prospect has raised concerns about the emergence of an exceptionally comprehensive surveillance regime, in which the individual's autonomy could be increasingly subordinated to the interests of the one-party state. The idea of a "mother of all surveillance states" emerged as a source of profound concern. Indeed, the investor and open-society champion, George Soros, has warned that such a system could place individual lives and freedom under the control of a totalitarian state. He argued that such a system would risk subordinating

[313] M. Bukhari, S. Anwar, *AI-Powered Surveillance in China and Its Implications for Global Democracy*, 2025, p. 72.
[314] Ivi p. 73.

personal autonomy and individual rights to the interests of the state in an unprecedented way in history.[315]

The analysis conducted in this section has revealed that, despite the existence of regulatory frameworks which formally seem to guarantee fundamental rights similarly to European standards, a significant gap emerges when considering their practical application. In the Chinese context, the extensive powers granted to the state, in conjunction with the pervasive deployment of AI-driven surveillance systems and their integration into law enforcement practices, substantially limit the effective guarantee of such rights. Therefore, the protection of individual rights, including the right to privacy, is largely subordinated to the imperatives of state control and social order.

3.4 European, American and Chinese regulatory approach: a comparative analysis

The detailed analysis of the legal systems of the European Union, the United States, and the People's Republic of China conducted in this chapter suggests that the regulation of AI, particularly of the emotion recognition systems, is not only a technological challenge but also a geopolitical and ideological extension of the constitutional and cultural values embedded in each national system. Although all three models face the risks arising from the advent of the digital society and the algorithmic processing of mass biometric data, their regulatory approaches differ significantly in terms of ideological assumptions, governance objectives, and the level of protection afforded to the individual's most private sphere.

The European regulatory framework is characterized by a right-based system, grounded in the protection of human dignity and fundamental rights. Within this framework, the safeguard of emotional privacy and informational privacy finds its core value in Article 8 of the ECHR, which guarantees respect for private life. As demonstrated by the evolution of the jurisprudence of the European Court of Human Rights, this concept has undergone an evolving process, by moving from its original negative notion of the "right to be left alone" to encompass physical, psychological, and moral integrity, as well as identity and the development of personality.

[315] M. Pei, *The Sentinel State: Surveillance and the Survival of Dictatorship in China*, 2024, p. 1,2,3.

The case law analyzed in the first chapter illustrates the gradual development of legal boundaries against technological intrusion. *S. and Marper v. The United Kingdom* (2008) established the principles of proportionality and necessity regarding biometric data. *Bărbulescu v. Romania* (2017) broadened the scope of Article 8 to cover horizontal relationships between private individuals, thus establishing that employers' monitoring must be subject to strict requirements regarding transparency and prior notice. Lastly, *Big Brother Watch and Others v. The United Kingdom* (2021) redefined the limits of mass surveillance, while *Glukhin v. Russia* (2023) directly addressed live facial recognition systems, labeling them as highly intrusive tools capable of generating a chilling effect on democratic freedom.

From a legislative perspective, the EU Charter of Fundamental Rights reflects this development by clearly distinguishing between the right to privacy in Article 7 and the separate right to the protection of personal data in Article 8. GDPR further enforces an ex-ante data protection by classifying biometric data as "special categories of data" (Article 9) and enforcing general prohibition on their processing, while the Data Act empowers the user as an active agent in the portability and control of the generated data.

The AI Act stands out as the culmination of the European process of legal consolidation. It adopts a risk-based approach in order to prevent behavioral biases while prohibiting practices that are considered unacceptable according to European Union values. The Regulation directly addresses emotion recognition systems, which aim to identify or infer emotions or intentions from biometric data and highlights the inherent danger of drawing inferences between physical signals and mental states. Consequently, Article 5 of the AI Act prohibits the use of emotion recognition systems in educational and workplace contexts, thus acknowledging the power asymmetry and the individual's inability to freely withdraw from algorithmic intrusion into their own inner self. When not prohibited, such systems are classified as "high-risk" (Article 6 and Annex III) in sensitive areas such as law enforcement imposing rigorous compliance requirements.

As analyzed in the first section of this chapter, this protective approach is reflected in the practices and decisions adopted at national level by individual European data protection authorities, which have established precise safeguards and bans against the use of biometric and emotion AI systems. The aim is to fully comply with the requirements set out in the AI Act to achieve harmonization across the European Union. The objective is to safeguard and

ensure fundamental human rights by managing innovation in the development of new AI-based technologies through the establishment of controlled and secured sandboxes, so as not to jeopardize citizens' fundamental rights.

In contrast to the mandatory European harmonization, the US model has historically been characterized by a market-oriented and structurally fragmented approach. The American conception of privacy is associated with the protection of the negative rights of the individual against state interference, rather than with the governance of private economic actors. Consequently, there is no comprehensive federal law on the protection of personal data or on the AI regulation. One of the most advanced attempts to fill this regulatory gap at state level is the California Privacy Rights Act (CPRA), which has introduced specific safeguards for consumers by codifying the category of sensitive personal information, which includes biometric and geolocation data. The CPRA grants California residents the right to restrict the use of such data and imposes transparency obligations regarding the algorithmic logic underlying automated decisions, namely profiling processes. However, unlike the AI Act, the CPRA fails to make any explicit reference to emotion recognition systems, thus leaving this technology without distinct regulatory measures.

At federal level, the Biden administration's initiatives, outlined in the *Blueprint for an AI Bill of Rights* (2022), have attempted to establish common principles drawn in part from the European model, such as privacy by design, transparency, purpose limitation and the need for free and informed consent. Nevertheless, the latest transition to the Trump administration revealed the vulnerability of a system based on executive orders and unstable political objectives, confirming the paramount importance of safeguarding private innovation and the free market at the expense of uniform protection of privacy rights. From the perspective of Article 8 ECHR, the American regulatory approach gives rise to significant concerns, as the pervasive deployment of emotion recognition technologies in sensitive areas such as workplace settings risks undermining the protection of individuals' rights, such as private life, personal dignity and freedom of expression. Consequently, by prioritizing market freedom and relying on fragmented state-level protections, the American model may fail to ensure an adequate level of protection for the right to private life, as required by Article 8 ECHR, particularly within contexts characterized by structural power imbalances.

Ultimately, the People's Republic of China adopts a regulatory model that diverges from both the European human-centered approach and American liberalism, as it is rooted in socialist tradition, a planned market economy, and collectivist cultural values in which the interests of the community have historically prevailed over individual autonomy. From a constitutional perspective, the 1982 Constitution offers limited safeguards. Although Article 33 affirms respect for human rights, Article 38 protects personal dignity and Article 35 guarantees civil liberties, there is no general right to privacy or data protection enshrined in the Constitution. Nevertheless, in light of the massive technological advances in the field of AI, the ongoing expansion of the market and the proliferation of the phenomenon of Big Data, China enacted the Personal Information Protection Law (PIPL) in 2021. As examined in the previous section of this chapter, from a terminological and structural perspective, the PIPL bears a striking resemblance to the European GDPR.

However, the fundamental discrepancy with the GDPR lies in the underlying political rationale. Whilst the European regulation aims to limit power imbalances by protecting individuals from both corporate entities and the state, the PIPL is specifically designed to address the excessive power of private technology companies in order to prevent anti-competitive practices, algorithmic discrimination and preserve social stability. This structural asymmetry is reflected in the most recent regulations, such as the *Measures for the Security Management of Facial Recognition Technology Applications* (2025). On the one hand, such measures impose strict restrictions on private individuals and commercial operators, requiring separate and explicit consent for the processing of facial features, prohibiting their installation in private areas of public spaces and obliging operators to provide non-biometric alternatives to consumers. On the other hand, in full accordance with Articles 26 and 35 of the PIPL, the same measures exclude public security authorities and law enforcement agencies from these restrictions as long as such systems are used for national security, crime prevention or the maintenance of public order.

Consequently, the technological infrastructure and the widespread use of predictive surveillance and emotion recognition systems are not merely limited practices but are institutionally legitimized. This is evidenced by international reports, such as the one published by ARTICLE 19 (2021), and by their implementation in monitoring practices, for instance in the Xinjiang region. Within this context, AI-driven systems stop being a potential threat to human rights and become an allied tool for the creation of the so-called Sentinel

State, thus subordinating the right to privacy to the State overarching needs to maintain centralized power, social and moral order though pervasive mass surveillance. In light of this, it can be affirmed that unlike the European framework, where privacy functions as a limit on state power, the Chinese model appears to subjugate individual privacy to collective and state interests, thereby undermining the balance between public authority and personal autonomy that lies at the core of Article 8 ECHR.

To better illustrate the differences between these three models that emerged as a result of the analysis carried out in this dissertation, a comparison table is provided below.

	European Union	**United States**	**China**
Conceptualization of Privacy	Fundamental human right	Protection primarily against state interference, with limited horizontal application	Seen in collective interest terms: means of social order
Regulatory framework	Comprehensive and harmonized system: CFREU, GDPR, Data Act, AI Act	Fragmented framework: absence of comprehensive federal law, reliance on sectoral and state-level regulations (e.g. CPRA and CAIA)	Centralized and state-driven framework: PIPL and targeted AI regulations (e.g. facial recognition measures)
Emotion recognition systems	AI Act and risk-based approach. Prohibition of their use in educational and workplace contexts due to	No explicit reference in regulations, nor prohibitions. Limited restrictions on private actors	Restrictions on private actors. Institutionalization of public authorities' use with minor restrictions

	power asymmetries.		
Enforcement and implementation	Enforcement through national Data Protection Authorities to achieve full harmonization. Support for innovation through regulatory sandboxes	Vulnerable to political transitions, relying on executive orders and shifting political objectives, leading to regulatory instability	Centralized and state-driven enforcement, supported by large-scale deployment of biometric surveillance technologies
Compatibility with Article 8 ECHR principles	High: Legal consolidation preventing biases and discrimination without jeopardizing citizens' fundamental rights	Partial and controversial: Paramount importance of private innovation and free market at the expense of uniform protection of privacy rights	Limited: systematic subordination of the right to privacy to the state's overarching needs, incompatible with Article 8 ECHR standards

Conclusion

This research explored the implications of emotion recognition systems in relation to the protection of fundamental human rights, with particular focus on the right to private life under Article 8 ECHR. Furthermore, it investigated how different jurisdictions deal with the challenges posed by the development of such technologies. The findings reveal that emotion recognition practices represent more than mere technological innovation, as they entail a qualitative change in the ways individuals can be monitored, assessed and ultimately influenced. The present dissertation highlights how emotion recognition systems interfere considerably with the right to privacy. Indeed, their distinctive feature lies in their ability to infer individuals' emotional states, as well as involuntary physical responses associated with those states on the basis of observable data such as facial expressions, vocal patterns, and other behavioral indicators. Such inferential ability extends beyond the scope of data collection and monitoring, entering a sphere that is considered inherently personal and private.

Consequently, the intrusion into an individual's private life is not limited to the gathering of externally observable information alone. Rather, it involves the interpretation of an individual's inner sphere. This raises significant concerns in light of Article 8 ECHR, particularly when such technologies are deployed in contexts where individuals do not have full awareness of their use and are unable to provide informed consent. As a result, the opaque nature of these systems combined with the imbalance of power between their deployers and the individuals subject to them further increases the potential risks, potentially undermining personal autonomy, dignity and private life.

Alongside this, the comparative analysis further shows significant divergences between the European model and the approaches adopted in other legal systems. The European Union has developed a regulatory framework centered on fundamental human rights, thus seeking to impose limitations and, in certain cases, prohibitions on the use of emotion recognition systems through measures such as the GDPR and ultimately the AI Act. This approach reflects a common and shared human-centric vision, aimed at preventing technological applications that may pose unjustified and disproportionate risks to individuals' rights.

By contrast, the United States is characterized by a fragmented and market-oriented regulatory landscape, where the lack of a comprehensive federal framework results in a less effective form of oversight and protection. On the other hand, the People's Republic of China integrates such technologies into a state governance system, in which their use aligns with social management and public security objectives.

It can be concluded that the differences observed are not merely formal, but result in fundamentally distinct practical implications, particularly in terms of the level of protection afforded to individuals' privacy rights and the degree of acceptance of intrusive forms of surveillance. Based on the findings emerging from this research, it is evident that emotion recognition systems challenge current legal frameworks, thus requiring a constant process of adaptation. This dissertation inevitably opens to future research, which is essential to understanding how these technologies will evolve and whether current regulatory responses will remain adequate. In particular, it will be relevant to assess whether the European model will be able to extend its reach beyond the European Union's borders, thus influencing global standards, or whether it will remain limited to a narrow domestic environment. At the same time, further technological developments may require the European Union itself to strengthen its current regulatory approach in order to ensure that the safeguards provided for in Article 8 ECHR are not progressively undermined or threatened.

Bibliography

Article 19. *Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights*. London: ARTICLE 19, 2021.

Aveni Alessandro. "The New Artificial Intelligence (AI) Italian Regulation Approved on 17th of September 2025: A Discussion". *Revista Processus de Estudos de Gestão, Jurídicos e Financeiros* 16, no. 51, 2025.

Barrett Lisa Feldman, Adolphs Ralph, Marsella Stacy, Martinez Aleix, and D. Pollak Seth. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements". *Psychological Science in the Public Interest* 20, no. 1, 2019.

BEUC (Bureau Européen des Unions de Consommateurs). *A European Strategy for Data: BEUC's Response to Public Consultation*. Ref: BEUC-X-2020-046, Brussels: BEUC, 2020.

Bishay Mina, Preston Kenneth, Strafuss Matthew, Page Graham, Turcot Jay, and Mavadati Mohammad. "AFFDEX 2.0: A Real-Time Facial Expression Analysis Toolkit". *Proceedings of the 2023 IEEE 17th International Conference on Automatic Face and Gesture Recognition (FG)*, IEEE, 2022.

Boyd Karen L., and Andalibi Nazanin. "Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work". *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1: Article 95, 2023.

Bukhari Munazzah, and Anwar Sadia. "AI-Powered Surveillance in China and Its Implications for Global Democracy". *Journal of Development and Social Sciences* 6, no. 2, 2025.

Calvo Rafael A., and D'Mello Sidney. "Affect Detection: An Interdisciplinary Review of Models, Methods, and Their Applications". *IEEE Transactions on Affective Computing* 1, no. 1, 2010.

China. *Constitution of the People's Republic of China* (1982, as amended in 2018), Translated by Changhao Wei and Taige Hu, *NPC Observer*, 2018.

China. Cyberspace Administration of China, and Ministry of Public Security. *Measures for the Security Management of Facial Recognition Technology Applications*, Beijing, issued March 13, 2025.

China. Ministry of Industry and Information Technology, Office of the Central Cyberspace Affairs Commission, National Development and Reform Commission, and Standardization Administration of China. *Guidelines for the Construction of a Comprehensive Standardization System for the National Artificial Intelligence Industry*, Beijing, Issued June 5, 2024.

China. National People's Congress of the People's Republic of China. *Personal Information Protection Law of the People's Republic of China*, President's Order No. 91, adopted August 20, 2021, effective November 1, 2021.

China. State Council of the People's Republic of China. *New Generation of Artificial Intelligence Development Plan*. State Council Document, 2017, No. 35. Translated by The Foundation for Law and International Affairs (FLIA), Washington DC, 2017.

Colangelo Giuseppe. *European Proposal for a Data Act – A First Assessment*. CERRE Assessment Paper, Brussels: Centre on Regulation in Europe (CERRE), 2022.

Costa Helena, and Mendonça Joana. "Assessing European Union Member States' Implementation of the Artificial Intelligence Act". *Human-Centred Technology Management for a Sustainable Future. Vol. 2: Technologies for a Sustainable Future, Proceedings of the 33rd IAMOT Conference, Porto, Portugal, 2024*, edited by Ricardo Zimmermann, José Coelho Rodrigues, Ana Simoes, Gustavo Dalmarco. Springer Proceedings in Business and Economics, Cham: Springer, 2024.

Costa Williams, Talavera Estefania, Oliveira Renato, Figueiredo Lucas, Teixeira João Marcelo, Lima João Paulo, and Teichrieb Veronica. "A Survey on Datasets for Emotion Recognition from Vision: Limitations and In-the-Wild Applicability". *Applied Sciences* 13, 2023.

Council of Europe. European Court of Human Rights. *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence*. Strasbourg: Council of Europe, 2017.

Council of Europe. *Convention 108+: Convention for the Protection of Individuals with regard to the Processing of Personal Data*. European Treaty Series, no. 223. Strasbourg: Council of Europe, 2018.

Crawford Kate, Dobbe Roel, Dryer Theodora, Fried Genevieve, Green Ben, Kaziunas Elizabeth, Kak Amba, Mathur Varoon, McElroy Erin, Nill Sánchez Andrea, Raji Deborah, Rankin Joy Lisi, Richardson Rashida, Schultz Jason, Myers West Sarah, and Whittaker Meredith. *AI Now 2019 Report*. New York: AI Now Institute, 2019.

Davis Wright Tremaine LLP. *Cal. Civ. Code § 1798.100 et seq., as amended* (California Civil Code Section 1798.100 et seq., as amended). Compliance Guide, Seattle, WA: Davis Wright Tremaine LLP, 2020.

De Hert Paul, and Gutwirth Serge. “Privacy, data protection and law enforcement. Opacity of the individual and transparency of power”. *Privacy and the criminal law*, E. Claes, A. Duff & S. Gutwirth. Antwerp/Oxford, Intersentia, 2006.

Del Gatto Sveva. "Facial Recognition Through the Lens of National Legislations - Italy". *European Review of Digital Administration & Law - ERDAL* 6, no. 1, 2025.

Denaro Fabrizio. "Artificial Intelligence Governance in Public Administration: National Regulatory Approaches in Italy and Spain under the EU AI Act”. SSRN Working Paper, 2025.

Deshmukh Renuka S., and Jagtap Vandana. "A Survey: Software API and Database for Emotion Recognition”. *Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, IEEE, 2017.

Di Salvo Michele. "Critical View of the Introduction of Artificial Intelligence in the Administrative Procedure: Reception of the EU AI Act in Italy". *Digital Law Journal* 6, no. 2, 2025.

European Confederation of Institutes of Internal Auditing. *The AI Act: Road to Compliance – A Practical Guide for Internal Auditors*. Brussels: ECIIIA, 2025.

European Court of Human Rights. *Grand Chamber Judgment in the Case of Bărbulescu v. Romania (Application no. 61496/08): Questions and Answers*. Strasbourg: Council of Europe, 2017.

European Data Protection Supervisor (EDPS). "Facial Emotion Recognition". *TechDispatch*, no. 1, 2021.

European Parliament and Council of the European Union. “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts”. *Official Journal of the European Union*, OJ L, 2024/1689, July 12, 2024.

European Union. *Charter of Fundamental Rights of the European Union (2000/C 364/01)*. 18 December 2000.

European Union. “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". *Official Journal of the European Communities* L 281, November 23, 1995.

European Union. "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)". *Official Journal of the European Union* L 119, May 4, 2016.

European Union Agency for Fundamental Rights (FRA). *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*. Luxembourg: Publications Office of the European Union, 2020.

European Union Agency for Fundamental Rights, Council of Europe. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018.

Fernández-Prados Juan S., Cara-Fernández Yolanda, Torres-Haro, and María J. "Racial/Ethnic Bias in AI Systems: A PRISMA Systematic Review of Magnitude, Domains, and Mitigation Strategies (2014–2025)". *International Journal of Migration Studies* 15, no. 1, 2025.

Floridi Luciano, Cowls Josh, Beltrametti Monica, Chatila Raja, Chazerand Patrice, Dignum Virginia, Luetge Christoph, Madelin Robert, Pagallo Ugo, Rossi Francesca, Schafer Burkhard, Valcke Peggy, and Vayena Effy. "AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations". *Minds and Machines* 28, no. 4, 2018.

Froomkin A. Michael. "The Death of Privacy?". *Stanford Law Review* 52, no. 5, 2000.

García-Hernández Rosa A., Luna-García Huizilopoztli, Jose M. Celaya-Padilla, García-Hernández Alejandra, Reveles-Gómez Luis C., Luis Alberto Flores-Chaires, Delgado-Contreras J. Ruben, Rondon David, and Villalba-Condori Klinge O. "A Systematic Literature Review of Modalities, Trends, and Limitations in Emotion Recognition, Affective Computing, and Sentiment Analysis". *Applied Sciences* 14, no. 16, 2024.

Gendron Maria, Roberson Debi, van der Vyver Jacoba M., and Barrett Lisa Feldman. "Perceptions of Emotion From Facial Expressions Are Not Culturally Universal: Evidence From a Remote Culture". *Emotion* 14, no. 2, 2014.

Guo Runfang, Guo Hongfei, Wang Liwen, Chen Mengmeng, Yang Dong, and Li Bin. "Development and Application of Emotion Recognition Technology—A Systematic Literature Review". *BMC Psychology* 12, 2024.

Gupta Uma G., and Ashok Gupta. "Vision: A Missing Key Dimension in the 5V Big Data Framework". *Journal of International Business Research and Marketing* 1, no. 3, 2016.

Han Shengnan, Nikou Shahrokh, and Ayele Workneh Yilma. "Digital Proctoring in Higher Education: A Systematic Literature Review". *International Journal of Educational Management* 38, no. 1, 2024.

Häuselmann Andreas N., Sears Alan M., Zard Lex, and Fosch-Villaronga Eduard. "EU Law and Emotion Data". *Proceedings of the 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII)*. IEEE, 2023.

High-Level Expert Group on Artificial Intelligence (AI HLEG). *Ethics Guidelines for Trustworthy AI*. Brussels: European Commission, 2019.

Hildebrand Mireille. *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press, 2020.

Hofstede Geert. "Dimensionalizing Cultures: The Hofstede Model". *Online Readings in Psychology and Culture* 2, no. 1, 2011.

Hoofnagle Chris Jay, van der Sloot Bart, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means". *Information & Communications Technology Law* 28, no. 1, 2019.

Italy. Garante per la protezione dei dati personali (Italian Data Protection Authority). *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021 [9703988]* (Injunction order against Luigi Bocconi

Commercial University of Milan - September 16, 2021 [9703988]). Provision n. 317, 2021.

Italy. Presidenza del Consiglio dei Ministri, Dipartimento per il programma di governo. *Focus: Analisi del quadro normativo in materia di Intelligenza artificiale* (Focus: Analysis of the regulatory framework on Artificial Intelligence). Rome: Presidenza del Consiglio dei Ministri, 2025.

Italy. Senato della Repubblica. *Disegno di Legge n. 1146: Disposizioni e deleghe al Governo in materia di intelligenza artificiale* (Bill No. 1146: Provisions and delegations to the Government regarding artificial intelligence). Approved March 20, 2025.

Jack Rachael E., Garrod Oliver G. B., Yu Hao, Caldara Roberto, and Schyns Philippe G. "Facial Expressions of Emotion Are Not Culturally Universal". *Proceedings of the National Academy of Sciences* 109, no. 19, 2012.

Jiang Lingjie. "The Current Situation and Risk Prevention of Facial Recognition Technology in China: A Legal and Governance Perspective". *Modern Law Research* 6, no. 4, 2025.

Keltner Dacher, Tracy Jessica L., Sauter Disa, and Cowen Alan. "What Basic Emotion Theory Really Says for the Twenty-First Century Study of Emotion". *Journal of Nonverbal Behavior* 43, no. 2, 2019.

Kerber Wolfgang. "Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives". *GRUR International*, 2022.

Khan Abdus Samad, Gul Rizwana, Naznin Shaista, and Khan Yunas. "The Right to Privacy, Its Progress & Decline: A Critical Review". *Journal of Business and Social Review in Emerging Economies* 8, no. 2, 2022.

Kilkelly Ursula. *The Right to Respect for Private and Family Life: A Guide to the Implementation of Article 8 of the European Convention on Human Rights*. Human Rights Handbooks, no. 1. Strasbourg: Council of Europe, 2001.

Landowska Agnieszka, Brodny Grzegorz, and Wrobel Michal R. "Limitations of Emotion Recognition from Facial Expressions in e-Learning Context". *Proceedings of the 9th International Conference on Computer Supported Education (CSEDU 2017)*, Vol. 2, SCITEPRESS – Science and Technology Publications, 2017.

Laskowska Marzena. *Artificial Intelligence in the Work of EU National Parliaments and the European Parliament: Survey Report*. Bureau of Research, Chancellery of the Sejm, 2025.

Levin Avner, and Jo Nicholson Mary. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground". *University of Ottawa Law & Technology Journal* 2, no. 2, 2005.

Li Shan, and Deng Weihong. "Deep Facial Expression Recognition: A Survey". *IEEE Transactions on Affective Computing*, 2020.

Li Tiffany, Bronfman Jill, and Zhou Zhou. "Saving Face: Unfolding the Screen of Chinese Privacy Law". *Boston University School of Law Faculty Scholarship*, Paper 533, 2018.

Lubello Valeria. "From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer". *DPCE Online* 69, no. 1, 2025.

Lynskey Orla. "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order". *International and Comparative Law Quarterly* 63, no. 3, 2014.

Mantelero Alessandro. "The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics". *Computer Law & Security Review* 30, no. 6, 2014.

Mattioli Michele, and Cabitza Federico. "Not in My Face: Challenges and Ethical Considerations in Automatic Face Emotion Recognition Technology". *Machine Learning and Knowledge Extraction* 6, no. 4, 2024.

McStay Andrew. *The Right to Privacy in the Age of Emotional AI*. Research Report for the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2020.

Murrugarra-Llerena Jeffri, Kirsten Lucas N., and Jung Claudio R. "Can We Trust Bounding Box Annotations for Object Detection?". *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2022.

Nartey Josephine. "The Ethics of Emotion Recognition Technology: Implications for Privacy and Consent". *SSRN Electronic Journal*, 2023.

OECD. *Progress in Implementing the EU Coordinated Plan on AI*. Vol. 1, Spain, 2025.

Organisation for Economic Co-operation and Development (OECD). *The OECD Privacy Framework*. Paris: OECD, 2013.

Orlando Alberto. "La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea iacta est?". *DPCE Online* 64, no. 2, 2024.

Palmiotto Francesca. "The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation". *European Journal of Risk Regulation* 16, 2025.

Pech Laurent. *The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU*. Brussels: Open Society European Policy Institute, 2021.

Pei Minxin. *The Sentinel State: Surveillance and the Survival of Dictatorship in China*. Cambridge, MA: Harvard University Press, 2024.

Petrucco Fabrizio. "The Right to Privacy and New Technologies: Between Evolution and Decay". *MediaLaws: Rivista di diritto dei media*, no. 1, 2019.

Picard Rosalind Wright. "Affective Computing". MIT Media Laboratory Perceptual Computing Section Technical Report, no. 321. Cambridge, MA: Massachusetts Institute of Technology, 1995.

Picard Rosalind Wright. *Affective Computing*. Cambridge, MA: MIT Press, 1997.

Pusztahelyi Réka. "Emotional AI and Its Challenges in the Viewpoint of Online Marketing". *Curentul Juridic* 23, no. 2, 2020.

Qian Cheng, Lobo Marques, and João Alexandre. "Consumer Response Analysis with AI and Facial Expression Recognition in Retail". *ICEME '25: Proceedings of the 2025 16th International Conference on E-business, Management and Economics*. New York, NY: ACM, 2025.

Rhue Lauren. "Racial Influence on Automated Perceptions of Emotions". *SSRN Electronic Journal*, 2018.

Roemmich Kat, Schaub Florian, and Andalibi Nazanin. "Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy". *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Article no. 550. New York: ACM, 2023.

Rouast Philipp V., Adam Marc T. P., and Chiong Raymond. "Deep Learning for Human Affect Recognition: Insights and New Developments". *IEEE Transactions on Affective Computing* 12, no. 2, 2021.

Samuelsson Lars, Coppélie Cocq, Stefan Gelfgren, and Jesper Enbom. *Everyday Life in the Culture of Surveillance*. Göteborg: Nordicom, University of Gothenburg, 2023.

Sarker Iqbal H. "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions". *SN Computer Science* 2, 2021.

Sartor Giovanni. *Artificial Intelligence: Challenges for EU Citizens and Consumers*. Briefing, Brussels: European Parliamentary Research Service (EPRS), 2019.

Sethu Vidhyasaharan, Provost Emily Mower, Epps Julien, Busso Carlos, Cummins Nicholas, and Narayanan Shrikanth. "The Ambiguous World of Emotion Representation". *arXiv preprint arXiv:1909.00360*, 2019.

Sbailò Ciro. "Executive Order 14110 Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth". *Diritto Pubblico Comparato ed Europeo* 26, no. 1, 2024.

Schabas William A. *The European Convention on Human Rights: A Commentary*. Oxford: Oxford University Press, 2015.

Shipman & Goodwin LLP. *California Privacy Rights Act: A Compliance Guide*. Hartford, CT: Shipman & Goodwin LLP, 2021.

Shorten Connor, and Khoshgoftaar Taghi M. "A Survey on Image Data Augmentation for Deep Learning". *Journal of Big Data* 6, no. 1, 2019.

Spain. Agencia Española de Protección de Datos (AEPD). *Resolución de Terminación del Procedimiento por Pago Voluntario* (Resolution on termination of the procedure due to voluntary payment). Enforcement Proceeding No. PS/00120/2021, Madrid: AEPD, 2021.

Thouvenin Florent. "Informational Self-Determination: A Convincing Rationale for Data Protection Law?". *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law* 12, no. 4, 2021.

United States. Office of the President. "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.". *Federal Register* 88, no. 210, November 1, 2023.

United States. White House Office of Science and Technology Policy (OSTP). *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*. Washington, DC: White House, 2022.

United Kingdom. *Data Protection Act 1998*. Public General Acts, c. 29, London: The Stationery Office, 1998.

Van der Sloot Bart. "A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle". *Computer Law & Security Review* 34, 2018.

Van der Sloot Bart. "The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases". *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law* 11, 2020.

Van der Sloot Bart, and Sacha van Schendel. *International and Comparative Legal Study on Big Data*. WRR Working Paper, no. 20. The Hague: Netherlands Scientific Council for Government Policy, 2016.

Vogiatzoglou Plixavra, and Valcke Peggy. "Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law". *Research Handbook on EU Data Protection Law*, edited by Eleni Kosta, Ronald Leenes, Irene Kamara, Cheltenham: Edward Elgar Publishing, 2022.

Weber Valentin. "China's AI-Powered Surveillance State". *Journal of Democracy* 36, no. 4, 2025.

Whitman James Q. "The Two Western Cultures of Privacy: Dignity Versus Liberty". *The Yale Law Journal* 113, no. 6, 2004.

Wilhelm Ernst Oliver, and Marc Bellon. *Early Compliance & Proactive Commitments: An Introduction to the EU AI Pact*. Micro-Insight Series, CEDPO AI and Data Working Group, 2024.

Zhang Yi-Chen. "China's Personal Information Protection Law (PIPL) 2021: An Analysis". *Modern Jurisprudence* 3, no. 3, 2025.

Zhang Yueming. "Personal Data Protection and Data Transfer Regulation in China". *Brussels Privacy Hub Working Paper Series* 10, no. 3. Brussels Privacy Hub, 2024.

Zuboff Shoshana. "Surveillance Capitalism and the Challenge of Collective Action". *New Labor Forum* 28, no. 1, 2019.

Case Law European Court of Human Rights

European Court of Human Rights, *Bărbulescu v. Romania*. Application no. 61496/08, Judgment of September 5, 2017, HUDOC database.

European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom*. Application nos. 58170/13, 62322/14, and 24960/15, Judgment of May 25, 2021. HUDOC database.

European Court of Human Rights, *Glukhin v. Russia*. Application no. 11519/20, Judgment of July 4, 2023. HUDOC database.

European Court of Human Rights, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of December 4, 2008, HUDOC database.

Sitography

AESIA. *Compliance Guides for the AI Act*, 2026, available at https://aesia.digital.gob.es/en/guides, accessed 11 May 2026.

CNIL. *AI system development: CNIL's recommendations to comply with GDPR*, 2026, available at https://www.cnil.fr/en/ai-system-development-cnils-recommendations-to-comply-gdpr, accessed 10 May 2026.

CNIL. *Hidden cameras: the CNIL sanctions the SAMARITAINE*, 2025, available at https://www.cnil.fr/en/hidden-cameras-cnil-sanctions-samaritaine accessed 11 May 2026.

CNIL. *The CNIL's missions*, 2025, available at https://www.cnil.fr/en/cnil/cnils-missions, accessed 10 May 2026.

Colorado General Assembly. *SB24-205: Consumer Protections for Artificial Intelligence*, available at https://leg.colorado.gov/bills/sb24-205 , accessed 16 May 2026.

Colorado Senate Bill 24-205. Enacted by the General Assembly of the State of Colorado, *Concerning Consumer Protections in Interactions with Artificial Intelligence Systems*, adding Part 17 to Article 1 of Title 6 of the Colorado Revised Statutes (codified as Colo. Rev. Stat. § 6-1-1701 *et seq.*), available at https://leg.colorado.gov/bills/sb24-205 , accessed 16 May 2026.

Council of Europe (n.d.). *Convention 108 and Protocol*, available at https://www.coe.int/en/web/data-protection/convention108-and-protocol accessed 9 February 2026, accessed 9 February 2026.

E-Learning Quality Network (ELQN). *The Power of Proctoring: Enhancing Knowledge Assessment in Online Education*, 2025, available at https://elqn.org/the-power-of-proctoring-enhancing-knowledge-assessment-in-online-education/, accessed 15 May 2026.

European Data Protection Supervisor. (n.d.). *Big data and the Digital Clearing House*. https://www.edps.europa.eu/data-protection/data-protection/reference-library/big-data-and-digital-clearing-house_en, accessed 9 February 2026.

Garante per la protezione dei dati personali. *L'Autorità - Chi siamo* (The Authority - Who we are), available at https://www.garanteprivacy.it/home/autorita, accessed 10 May 2026.

Garante per la protezione dei dati personali. *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani,* 2022, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323, accessed 10 May 2026.

Healthy Mind. *Neuromind: The Alliance of Neuroscience and AI*, 2026, available at https://healthymind.fr/en/solution-neuromind/, accessed 14 April 2026.

OECD. *About the OECD*, 2026, available at https://www.oecd.org/en/about.html, accessed 11 May 2026.

Open Society Justice Initiative. (n.d.). *Big Brother Watch v. United Kingdom*, https://www.justiceinitiative.org/litigation/big-brother-watch-v-united-kingdom, accessed 4 February 2026.

Regulations.ai. *Spain – AI Governance Bill, Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial, Draft Bill for the Good Use and Governance of Artificial Intelligence,* 2025, available at https://regulations.ai/regulations/RAI-ES-NA-DADLGXX-2025, accessed 11 May 2026.

ScienceDirect. *Physiological Signal - an overview*, n.d., available at https://www.sciencedirect.com/topics/computer-science/physiological-signal, accessed 14 April 2026.

Valín Elena, and Oriol Rebeca. *New AESIA Guidelines to support compliance with the AI Act*, 2026, available at https://www.hsfkramer.com/notes/madrid/2026-posts/ebulletin-new-aesia-guidelines-to-support-compliance-with-the-ai-act-february-2026, accessed 11 May 2026.

White House. *National Security Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing AI to Achieve National Security Objectives; and Mitigating Risks from Adversary Use of AI*, October 24, 2024, available at https://www.presidency.ucsb.edu/documents/national-security-memorandum-advancing-the-united-states-leadership-artificial, accessed 17 May 2026.