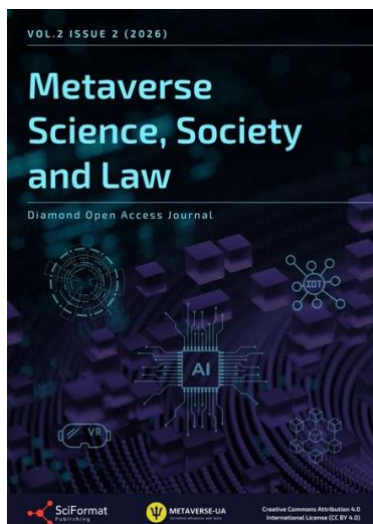




Metaverse Science, Society and Law

Vol. 2, Issue 3 (2026)



Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
✉ editorial-office@sciformat.ca

ARTICLE TITLE

UNIQUE IDENTIFICATION UNDER THE GDPR AND MEMBER
STATE LAW: THE CASE OF SPAIN

DOI

<https://doi.org/10.69635/mssl.2026.2.3.56>

RECEIVED

22 April 2026

ACCEPTED

19 August 2026

PUBLISHED

31 August 2026

LICENSE



The article is licensed under a **Creative Commons Attribution 4.0 International License**.

© The author(s) 2026.

This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

UNIQUE IDENTIFICATION UNDER THE GDPR AND MEMBER STATE LAW: THE CASE OF SPAIN

Daria Bulgakova

Advocate, PhD in International Law, Kryvyi Rih, Ukraine; Associate Professor, Department of Law and Public Administration, Zaporizhzhia Institute of Economics and Information Technologies, Zaporizhzhia, Ukraine
ORCID ID: 0000-0002-8640-3622

Hanna Hulievska

PhD in Law, Associate Professor, Head of the Department of Law and Public Administration, Zaporizhzhia Institute of Economics and Information Technologies, Zaporizhzhia, Ukraine
ORCID ID: 0000-0001-7643-8162

ABSTRACT

The study infers that biometric access control systems, including facial recognition and fingerprint verification, involve the processing of special categories of personal data under Articles 4(14) and 9 of the General Data Protection Regulation whenever they facilitate or substantiate the unique identification of individuals. The distinction between biometric identification (1:N) and verification (1:1) does not exclude the relevance of Article 9 GDPR if tag effects arise.

Generic requests of public interest or security objectives are low to justify such processing under Article 9(2)(g) GDPR.

Spanish constitutional doctrine and EU data protection law direct that a law of acceptable rank establish any hindrance of the fundamental right to data protection, clearly express the substantial public welfare pursued, and provide precise, foreseeable, and robust safeguards.

The research finds that Article 13(1) of Spanish Law 19/2007 does not meet these requirements, as it neither expressly authorizes the processing of biometric data nor establishes appropriate safeguards. National regulation and administrative measures mandating biometric access systems in sports venues lack a valid legal basis under Article 9(2) GDPR and are incompatible with the EU data protection framework.

Decisions and prior consultations by the Agencia Española de Protección de Datos demonstrate strict enforcement of GDPR principles, including necessity, proportionality, transparency, and data minimisation. Biometric recognition was invariably considered unlawful due to the absence of a valid legal basis, invalid consent, lack of DPIAs, and the availability of less intrusive alternatives.

Therefore, the authors confirm that technical design choices do not alter the legal qualification of biometric data. Unique identification capability is decisive, and biometric systems must stay exceptional rather than authoritative means in access control practices.

KEYWORDS

Biometric Data, Personal Data Protection Law, Access Control, Supervisory Enforcement, Agencia Española de Protección de Datos, SIDECU, S.A., Burgos Club de Fútbol, S.A.D.

CITATION

Daria Bulgakova, Hanna Hulievska. (2026). Unique Identification Under the GDPR and Member State Law: The Case of Spain. *Metaverse Science, Society and Law*. Vol. 2, Issue 3. doi: 10.69635/mssl.2026.2.3.56

COPYRIGHT

© The author(s) 2026. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

Introduction

Within the European Union, biometric data occupy a distinct legal position under Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) (European Parliament & Council of the European Union, 2016). Biometric data for unique identification of a natural person is explicitly classified as a special category of personal data and prohibited in principle.

The author of that research stems from the **hypothesis** that the practice of biometric access control systems in sport public environments oftentimes fails to meet the strict legal requirements imposed by Articles 5, 9, and 35 of the GDPR, even when such systems are justified by reference to security, public interest, or technological safeguards. It is hypothesized that the distinction between biometric identification and biometric authentication is often misused to bypass the variety of unique identification through biometric data processing as special data category. Technical design features, likewise, encryption or non-storage of raw images do not neutralize the legal qualification of biometric templates as biometric personal data and may be insufficient to justify biometric processing under Article 9(2)(g) GDPR.

In this regard, the **purpose** of this research is a coherent legal assessment of biometric data processing under the GDPR with particular emphasis on fingerprint and facial recognition access control systems in sport under the exception of data protection law. The steps-forward are:

- to assess the legal concept of biometric data within the meaning of Articles 4(1) (14) GDPR;
- to discuss the conditions under which biometric processing may lawfully proceed under Article 9(2) GDPR, with a focus on the “substantial public interest” – “g” exception;
- to have a legal assessment of the enforcement practice of the Spanish Data Protection Authority in 2024 and 2025;
- to highlight the importance of necessity, proportionality, and Data Protection Impact Assessments in settling the lawfulness of biometric access control systems in sport;
- to contribute to the doctrinal debate on the limits of biometric normalization in everyday domains specifically during sport events.

Material and methods

The research is based on the following primary and secondary legal **materials**:

1. EU legal framework: mostly on the Regulation (EU) 2016/679 (GDPR) with a particular attention on Articles 4(1), 4(14), 5, 6, 9, 13, 35 and Recital 51; Guidelines on the use of facial recognition technologies (Council of Europe, 2021; (European Data Protection Board, 2023); Article 29 Working Party opinions (Article 29 Data Protection Working Party, 2007, 2012).
2. National Spanish law: Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) (Spain, 2018); Law 19/2007 of 11 July on measures against violence, racism, xenophobia, and intolerance in sport (Spain, 2007); Law 39/2015 on the Common Administrative Procedure of Public Administrations (Spain, 2015).
3. Supervisory authority practice: Advisory opinion 0098/2022 of the Spanish Data Protection Authority (AEPD, 2023); The Decision on Burgos Club de Fútbol, S.A.D. case (AEPD, 2024); The Decision on SIDECU S.A. case (AEPD, 2025).
4. Case law of the Spanish Constitutional Court concerning the fundamental right to data protection (Spanish Constitutional Court, 2019, 2000).

The research employs the following **methods**:

1. Doctrinal legal analysis to interpret legal provisions on biometric data.
2. Comparative interpretation between EU-level norms and Spanish national law to assess regulatory compatibility.
3. Case study method, examining the Spanish Data Protection Authority's practice to find out regulatory reasoning and compliance failures.
4. Proportionality and necessity assessment.
5. Functional analysis, concentrating on the actual capability of biometric systems (unique identification), rather than their technical design claims (encryption, absence of raw image storage).

Discussion

Biometric data processing under the GDPR. Biometric data processing systems are automated methods based on the processing of personal data relating to biometrical characteristics of natural persons through devices or sensors. Such processing results in the creation of biometric templates, which enable the identification.

As clarified by the Article 29 Working Party¹ on the concept of personal data (Article 29 Data Protection Working Party, 2007), biometric data may be defined as biological properties, physiological characteristics, behavioural traits, or deeply ingrained skills attributable to a single individual with a degree of probability. Typical examples include fingerprint and facial recognition.

For instance, the ePrivacy Directive (European Parliament & Council of the European Union, 2002) regulates the processing of personal data in the context of electronic communications, with a focus on confidentiality of communications, cookies, spam, traffic, and location data, and consent for storing or processing data. Although biometric data are not explicitly mentioned in this Directive, any biometric data, such as fingerprint or facial data that are collected, transmitted, or stored through electronic communication systems (for example, electronic ID systems, access control apps, or messaging platforms) are considered personal data. In such cases, the rules of the ePrivacy Directive on consent, confidentiality, and security apply in cross with the GDPR, which explicitly categorizes biometric data used for identification as a special category of personal data.

The GDPR codifies this understanding in Article 4(14), defining biometric data as personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person. This definition proposed to be read in conjunction with Article 4(1) of the GDPR, which links personal data to the possibility of identifying an individual, either directly or indirectly. Hence, biometric data qualify as personal data when three cumulative criteria are met:

- (1) Nature of the data - the data relate to physical, physiological, or behavioural characteristics of a natural person;
- (2) Purpose of processing - the data are used to allow or confirm the unique identification of that person;
- (3) Means of processing - the data are obtained through specific technical processing – automated - enabling such identification.

Biometric systems may operate either as (Article 29 Data Protection Working Party, 2012):

- (1) Identification systems (1:N), comparing a biometric sample against multiple stored templates; or
- (2) Verification/authentication systems (1:1), comparing a biometric sample against a single stored template.

While these systems differ technically and in their error rates, the GDPR treats both as biometric processing, where they conform to allow or confirm unique identification. The distinction between “allow” and “confirm” identification in Article 4(14) GDPR encompasses both identification and authentication mechanisms.

According to the European Data Protection Board (EDPB) Guidelines 05/2022 (2023) depart from the distinction between authentication/verification and identification in determining the processing of biometric data as a special category in para 12, - both scenarios involve the processing of special categories of data: "While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data". In this regard, the understanding that the processing of biometric data, whether in the context of authentication/verification or identification, constitutes the processing of special categories of data, subject to the general prohibition and exceptions under Article 9 GDPR.

¹ The Article 29 Data Protection Working Party (WP29) was established pursuant to Article 29 of Directive 95/46/EC as an independent European advisory body on data protection and privacy. Its ruling confined the provision of expert opinions, recommendations, and guidance aimed at ensuring a uniform application of EU data protection law across the Member States. The tasks of the Working Party were defined in Article 30 of Directive 95/46/EC and further specified in Article 15 of Directive 2002/58/EC (ePrivacy Directive). These tasks included advising the European Commission on matters relating to the protection of personal data, promoting consistent interpretation of data protection rules, and examining questions concerning the application of national measures adopted pursuant to EU data protection legislation. The secretariat of the Working Party was provided by Directorate C (Civil Justice, Rights and Citizenship) of the Directorate-General for Justice, Freedom and Security of the European Commission, with its seat in Brussels, Belgium. Following the entry into force of the GDPR, the Article 29 Working Party was replaced by the European Data Protection Board (EDPB) pursuant to Article 68 GDPR. Still, the opinions and guidelines adopted by the WP29 remain of interpretative relevance, particularly where GDPR provisions codify or build upon concepts developed under Directive 95/46/EC.

This a decisive clarification concerns the legal nature of biometric templates. Raw biometric data (such as a facial image scan) constitutes personal data under Article 4(1) GDPR. However, they qualify as biometric data under Article 4(14) (European Parliament & Council of the European Union, 2016) only when they are subject to technical processing that produces a machine-interpretable biometric template. As clarified by Recital 51 GDPR (European Parliament & Council of the European Union, 2016) and by the Guidelines on Facial Recognition (Council of Europe, 2021), it is the biometric template, not the raw image, that constitutes the biometric personal data enabling automated identification. The fact that the original image is not stored does not negate the existence of biometric data processing where templates are generated, stored, and compared. Therefore, facial recognition access systems involve the processing of special category biometric data under Articles 4 (14) and 9 of the GDPR (European Parliament & Council of the European Union, 2016). Physical characteristics of individuals are technically processed to generate unique biometric templates that allow for identification. And, even if these templates are encrypted, encryption does not change their legal nature, since the system operator can decrypt them to verify a person's identity during each entry and exit.

Such processing includes multiple operations under Article 4 (2) GDPR (European Parliament & Council of the European Union, 2016):

- Collection and registration of facial samples.
- Generation of the biometric template.
- Storage and use within the system for access control.
- Recording of entry and exit times.

Besides, the system design itself is considered a processing operation and must comply with GDPR principles and obligations. Such processing is inherently regarded as high-risk processing within the meaning of Article 35 GDPR (European Parliament & Council of the European Union, 2016), demanding a Data Protection Impact Assessment (next in the text - DPIA).

Biometric access control systems meet several high-risk criteria simultaneously, including the processing of special category data, the use of biometric technologies, and the deployment of innovative technologies. It means, controllers intending to deploy biometric identification systems must, before processing, conduct a valid DPIA meeting the requirements of Article 35(7) GDPR (European Parliament & Council of the European Union, 2016), and including a necessity and proportionality check and an evaluation of less intrusive alternatives.

Biometric data processing according to the Spanish Data Protection Authority (AEPD, 2023). The Spanish Data Protection Authority (Agencia Española de Protección de Datos) (AEPD, 2023) held the guidance on the legal and regulatory requirements for implementing facial recognition systems in sports venues. The consultation raised the matter of whether the adoption of a resolution by the Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia (next in the text – CEVRXID) within the scope of its powers, establish measures requiring clubs to install biometric systems to control all access points to supporter sections, allowing the unequivocal identification of fans entering those areas, would be legally viable in accordance with data protection legislation. The power legally conferred by Article 13(1) of Law 19/2007 (Spain, 2007) which authorizes the Commission to decide on the implementation of additional security measures for sporting competitions or events classified as high risk, or for venues that have been subject to closure sanctions. This includes, in particular, the power to boost systems for verifying the identity of persons seeking access to sports venues.

On one hand, the processing of fans' personal data would be carried out pursuant to Article 6(1)(e) of GDPR, that is, the processing would be necessary "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (European Parliament & Council of the European Union, 2016). The explanation of this measure is the task carried out by the relevant clubs in the public interest that would guarantee the safety and integrity of persons attending football stadiums, as well as would prevent and avoid violations of fundamental rights, hate crimes, and discrimination through the aforementioned measures. The actual exception provided for in Article 9(2)(g) GDPR (European Parliament & Council of the European Union, 2016) would be relevant for the processing of biometric data when it "is necessary for reasons of substantial public interest, on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject" (European Parliament & Council of the European Union, 2016). In this regard, any resolution adopted by the CEVRXID would also establish the appropriate and specific measures that relevant clubs suggested to implement proportionality assessment, analyzing from a data protection perspective both the suitability of the measure,

the necessity of the processing, and its proportionality in the strict sense to protect the fundamental rights and interests of data subjects in connection with the implementation of the required additional measures, as directed by Article 9(2)(g) GDPR (European Parliament & Council of the European Union, 2016). At this point, the facial recognition would guarantee that the processing of identifying personal data together with biometric data by relevant clubs is carried out in full compliance as required by Article 5 GDPR (European Parliament & Council of the European Union, 2016).

The advisory consultation. The GDPR defines biometric data in Article 4(14) as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data” (European Parliament & Council of the European Union, 2016).

Article 9 of that Regulation governs the processing of special categories of data, including biometric data, establishing a general prohibition on their processing in the following terms: “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” (European Parliament & Council of the European Union, 2016).

With regard to the processing of biometric data analyzing Article 9(1) in conjunction with Recital 51 GDPR (European Parliament & Council of the European Union, 2016), as well as taking into account the Amending Protocol to the Convention 108+ (European Commission, 2018), the Spanish Data Protection Authority stated (AEPD, 2023): “In order to clarify interpretative doubts regarding the classification of biometric data as special categories of data, reference may be made to the distinction between biometric identification and biometric verification/authentication established in the Opinion 3/2012 (Article 29 Data Protection Working Party, 2012) on developments in biometric technologies: “Biometric identification: the identification of an individual by a biometric system is normally the process of comparing their biometric data (acquired at the time of identification) with a set of biometric templates stored in a database (i.e., a one-to-many matching process). Biometric verification/authentication: the verification of an individual by a biometric system is normally the process of comparing their biometric data (acquired at the time of verification) with a single biometric template stored on a device (i.e., a one-to-one matching process).”

This same distinction is reflected in the White Paper on Artificial Intelligence (European Commission, 2020): “With regard to facial recognition, ‘identification’ refers to the comparison of a person’s facial image template with many templates stored in a database to determine whether the image is present therein. ‘Authentication’ (or ‘verification’), by contrast, generally refers to matching two specific templates. It allows the comparison of two biometric templates that are presumed to belong to the same person, in order to determine whether the two images correspond to the same individual. This procedure is used, for example, in automated border control gates at airports”.

Therefore, the concept of biometric data encompasses both scenarios: identification and verification/authentication. However, as a general rule, biometric data will only be regarded as a special category of data where it is subject to technical processing aimed at biometric identification (one-to-many), and not in cases of biometric verification/authentication (one-to-one). In the present matter, the consultation refers to the processing of biometric data aimed at the unequivocal identification of a natural person and, accordingly, involves the processing of special categories of personal data. It is emphasized the difficulty of clearly distinguishing between identification and authentication, the need to assess each case individually based on the specific techniques used and the purpose of the processing, and the obligation to afford the highest level of protection to data subjects’ rights when using techniques that may be more intrusive to privacy and generate risks.

Article 9(2) (European Parliament & Council of the European Union, 2016) authorizes the processing of all such data when one of the ten circumstances listed therein applies (points (a) to (j)). Some of these circumstances have a limited scope of application (labour, social, associative, healthcare, judicial, etc.) or respond to a specific purpose and therefore, in themselves, delimit the specific processing operations they authorize as exceptions to the general rule. The enabling effect of several of the circumstances provided for therein is conditional upon them being expressly provided for and regulated by Union law or by the law of the Member States within their respective competences; this is the case for the circumstances set out in points (a), (b), (g), (h), (i) and (j). Thus, given that their processing is generally prohibited, any exception to this prohibition must be interpreted restrictively.

The question for further consideration is whether the processing of biometric data by facial recognition systems in online assessment processes could be justified by the existence of a substantial public interest under Article 9 (2) (g) GDPR: "(g) the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject" (European Parliament & Council of the European Union, 2016)?

The processing of personal data necessary for the provision of public interest is generally legitimized under Article 6 (1) (e) (European Parliament & Council of the European Union, 2016). However, for special categories of data, the provision in letter (g) of Article 9 (2) GDPR does not only refer to the existence of a public interest (as is the case in many other GDPR provisions) but is the only provision that requires the interest to be "substantial" qualifying the public interest due to the importance and need for heightened protection of the data processed. Important, this condition finds its precedent in Article 8 (4) of Directive 95/46/EC: "Member States may, where appropriate safeguards exist, provide for other exceptions for important reasons of public interest, beyond those in paragraph 2, either by national legislation or by decision of the supervisory authority" (European Parliament & Council of the European Union, 1995). However, the GDPR introduces stricter regulation by replacing "important" with "substantial" and by not allowing the exception to be set by supervisory authorities.

Regarding what constitutes a "substantial public interest," the case law of the European Court of Human Rights under Article 8 of the European Convention on Human Rights (European Commission, 2018) should also be considered. The Court has held that the processing of personal data constitutes a lawful interference with the right to respect for private life only if it is carried out in accordance with the law, serves a legitimate aim, respects the essence of fundamental rights and freedoms, and is necessary and proportionate in a democratic society to achieve a legitimate aim; the concept of necessity implies that the interference responds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.¹

The AEPD concluded that no legal provision in Spanish law met the requirements of Article 9 (2) (g) GDPR; therefore, processing could only be based on the free consent of the data subjects.²

The judgment of the Spanish Constitutional Court regarding restrictions on the fundamental right to personal data protection defining the fundamental right to personal data protection as an autonomous right empowering individuals to control which personal data they provide to third parties (state or private) and to know who holds such data and for what purpose, it analysed the limits of this right, stating: "...the right to data protection is not unlimited. Although the Constitution does not explicitly impose specific limits, nor refer to the Public Authorities for their determination as it does with other fundamental rights, such limits must be found in other constitutionally protected fundamental rights and legal interests, in accordance with the principle of constitutional unity."³ The essential point is that only the Law, and no other authority, may set limits to a fundamental right. Rights may yield to constitutionally relevant goods or interests, provided that such restriction is necessary, proportionate, and respects the essential content of the restricted right.⁴ Thus, if the Law merely empowers another public authority to set restrictions on fundamental rights on a case-by-case basis, the resulting rules may violate the right to data protection if applied inconsistently or without constitutional safeguards, affecting acquisition, storage, processing, and disclosure of personal data.

With regard to the right to the protection of personal data, it must be held that the constitutional legitimacy of restricting this right cannot be based solely on the activity of the public administration.⁵ Nor is it sufficient for the law to empower the administration to specify its limits on a case-by-case basis, merely indicating that such specification must occur when some constitutionally protected right or interest is present.

¹ See *D.L. v. Bulgaria*, no. 7472/14, 19 May 2016; *Dragojević v. Croatia*, no. 68955/11, 15 Jan 2015; *Peck v. UK*, no. 44647/98, 28 Jan 2003; *Leander v. Sweden*, no. 9248/81, 26 Mar 1987, among others.

² The AEPD also has investigated the national Report 36/2020 on the use of facial recognition in online assessment tests, attention should be paid to Report 31/2019 on the incorporation of facial recognition in video surveillance services under Article 42 of the Spanish Private Security Act, and Report 97/2020 on the Ministerial Order project concerning remote identification methods for issuing qualified electronic certificates.

³ SSTC 11/1981, 8 April, F.7; 196/1987, 11 Dec; and regarding Art. 18, STC 110/1984, F.5.

⁴ SSTC 57/1994, 28 Feb; 18/1999, 22 Feb.

⁵ The Constitutional Court of Spain ruled specifically on Article 9(2)(g) of the GDPR, as a result of the challenge to Article 58 bis of Organic Law 5/1985 of 19 June on the General Electoral Regime, introduced by the third final provision of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights. This provision concerned the lawfulness of the collection of personal data relating to individuals' political opinions carried out by political parties in the context of their electoral activities, and it was declared unconstitutional by Judgment No. 76/2019 of 22 May. That judgment first analyses the legal regime applicable to the processing of special categories of data under the GDPR.

It is the legislature that must determine when such a right or interest arises that justifies the restriction of the right to the protection of personal data and under what circumstances it may be limited, and it must do so through precise rules that make the imposition of such a limitation and its consequences foreseeable to the data subject.

The processing of special categories of personal data is one of the areas in which the General Data Protection Regulation has expressly recognized that Member States have a “margin of manoeuvre” to “specify their rules” as described in Recital 10 (European Parliament & Council of the European Union, 2016). This margin of legislative discretion extends both to the determination of the legal bases for processing particularly protected personal data namely, the identification of the essential public interest purposes and the assessment of the proportionality of the processing in relation to the pursued aim, while respecting the essence of the right to data protection and to the establishment of “appropriate and specific measures to safeguard the data subject’s fundamental rights and interests” according to the Article 9(2)(g) (European Parliament & Council of the European Union, 2016). The Regulation therefore contains a specific obligation for Member States to establish such safeguards when they authorize the processing of particularly protected personal data.

With regard to the first of the requirements laid down in Article 9(2)(g) the invocation of an essential public interest and the necessary specification thereof the Constitutional Court (Spanish Constitutional Court, 2000) rejected the possibility that the identification of the legitimate purposes of the restriction could be carried out by means of generic concepts or vague formulas, holding that the restriction of the fundamental right to the protection of personal data cannot be based solely on the generic invocation of an indeterminate “public interest.” It is rejected the identification of legitimate purposes through generic concepts or vague formulas.

In its Article 24(1) LOPD the expression ‘control and verification functions’ opens up such a broad space of uncertainty that it gives rise to a double and pernicious consequence. On the one hand, by authorizing the administration to restrict fundamental rights by invoking such an expression, the authority renounces fixing the limits itself and empowers the administration to do so. And it does so in such a way that it allows virtually all administrative activity to be subsumed under that expression, since any administrative activity that entails entering into a legal relationship with an individual which will be the case in practically all situations where the administration requires someone’s personal data will ordinarily involve the power of the administration to verify and control whether that individual has acted in accordance with the administrative legal regime governing the relationship entered into with the administration. This, in view of the ground for restricting the right to be informed under Article 5 LOPD, leaves the citizen in complete uncertainty as to when such a circumstance will arise (if not in all cases) and renders ineffective any mechanism of judicial protection that must assess such a restriction of fundamental rights without any complementary criterion to assist in controlling administrative action in this field.

The same criticisms apply to the use, in Article 24(2) LOPD, of the expression ‘public interest’ as the basis for imposing limits on the fundamental rights recognized in Articles 18(1) and 18(4) of the Constitution, as it entails an even greater degree of uncertainty; it suffices to note that all administrative activity ultimately pursues the safeguarding of general interests, the attainment of which constitutes the purpose that the administration must objectively serve pursuant to Article 103(1) of the Constitution (Spanish Constitutional Court, 2000).

Accordingly, it must likewise be concluded that the constitutional legitimacy of restricting the fundamental right to the protection of personal data cannot be based solely on the generic invocation of an indeterminate “public interest.” Otherwise, the legislature would have transferred to political parties, whom the challenged provision authorizes to collect personal data relating to individuals’ political opinions in the context of their electoral activities, the performance of a function that belongs exclusively to the legislature in matters of fundamental rights by virtue of the statutory reservation.

On the other hand, with regard to the safeguards that the legislature must adopt, Judgment recalling (Spanish Constitutional Court, 2019; Spanish Constitutional Court, 2000): “In view of the potential intrusive effects on the affected fundamental right resulting from the processing of personal data, the case-law of this Court requires the legislature, in addition to complying with the aforementioned requirements, also to establish appropriate technical, organizational, and procedural safeguards that prevent risks of varying probability and severity and mitigate their effects, since only in this way can respect for the essential content of the fundamental right itself be ensured.” Further it examines which rule must contain such safeguards: “Therefore, resolving the present challenge requires us to clarify a doubt raised regarding the scope of our doctrine on appropriate safeguards, namely, whether appropriate safeguards against the use of information technology must be contained in the very law that authorizes and regulates such use, or whether they may also be found in other

normative sources. The question can only have one constitutional answer. The provision of appropriate safeguards cannot be deferred to a moment subsequent to the legal regulation of the personal data processing in question. Appropriate safeguards must be incorporated into the legal regulation of the processing itself, either directly or by express and precisely delimited reference to external sources possessing the appropriate normative rank. Only such an understanding is compatible with the dual requirement deriving from Article 53(1) of the Constitution for the legislature with regard to fundamental rights: the statutory reservation for regulating the exercise of the fundamental rights recognized in Chapter II of Title I of the Constitution, and respect for the essential content of those fundamental rights. According to settled constitutional case-law, the statutory reservation does not merely require that a law authorize the restrictive measure affecting fundamental rights; it is also necessary, in accordance both with requirements sometimes described as normative predetermination and sometimes as quality of the law, and with respect for the essential content of the right, that the legislature - who bears the primary obligation to balance the competing rights or interests - predetermine the cases, conditions, and safeguards under which restrictive measures affecting fundamental rights may be adopted. This requirement of predetermination with respect to essential elements, ultimately also linked to the proportionality assessment of the limitation of the fundamental right, cannot be deferred to subsequent legislative or regulatory development, nor can it be left in the hands of private parties” (Spanish Constitutional Court, 2019, legal ground 8).

Therefore, the processing of biometric data under Article 9(2)(g) (European Parliament & Council of the European Union, 2016) requires that it shall be provided for a rule of European Union or national law, and such a rule has the rank of law. That law must also specify the essential public interest justifying the restriction of the right to the protection of personal data and the circumstances under which it may be limited, establishing precise rules that make the imposition of such a limitation and its consequences foreseeable to the data subject; the generic invocation of a public interest is not sufficient for these purposes. In spare, that law must establish appropriate technical, organizational, and procedural safeguards to prevent risks of varying probability and severity and to mitigate their effects.

Results

Pursuant to the powers conferred upon supervisory authorities under Article 58(2) of GDPR and in accordance with Articles 47, 48(1), 64(2) and 68(1) of Organic Law 3/2018 on the LOPDGDD (Spain, 2018), jurisdiction to initiate and resolve the present administrative proceedings lies with the AEPD.

Article 63(2) LOPDGDD provides that proceedings conducted by the AEPD shall be governed primarily by the GDPR and national data protection legislation, supplemented, where compatible, by the general rules on administrative procedure laid down in Law 39/2015 on the Common Administrative Procedure of Public Administrations (next in the text - LPACAP) (Spain, 2015).

Thus, the AEPD may initiate a sanctioning procedure against companies pursuant to Article 64 LOPDGDD (Spain, 2018), subject to a maximum duration of twelve months from the date of initiation, after which the proceedings lapse by operation of law. Let’s have a look on some of such proceedings.

The Facial Recognition in the Burgos Club de Fútbol (AEPD, 2024)¹. The current analysis is centred on the decision of the Spanish Data Protection Authority (Agencia Española de Protección de Datos, AEPD) in the case of Burgos Club de Fútbol, S.A.D., made on 9 April 2024.

According to the research (Bulgakova, 2025) on 4 November 2022, Burgos Club de Fútbol, S.A.D. implemented a biometric access control system requiring approximately 700 members of the club (including staff and players) to provide fingerprint data as a mandatory condition for accessing the supporters’ stand “La Hinchada del Arlanzón” at El Plantío Stadium. No alternative means of access were initially offered. The measure was justified by reference to an agreement adopted by the State Commission against Violence, Racism, Xenophobia, and Intolerance in Sport.

The biometric system, supplied by La Liga, processed fingerprint templates alongside additional personal data, including names, national identity document numbers, and identification codes. This system replaced a previous access regime based on the presentation of identity documents. Information regarding the new processing operation and its alleged legal basis was published on the website of the State Commission, rendering biometric processing de facto mandatory for access to the designated supporters’ area.

¹ This contribution is based on an empirical and doctrinal analysis conducted by Daria Bulgakova, which presented the results of the research at the scientific and practical conference dedicated to Europe Day (Kharkiv, 9 May 2025) and thereafter published as conference theses.

Complaints were submitted to the AEPD on 4 and 7 November 2022, alleging that the biometric processing was disproportionate and that data subjects had not been adequately informed in accordance with GDPR requirements. The system was first used in practice on 8 December 2022 during a football match. No minimum age threshold was established, enabling the processing of biometric data of minors, subject to parental or guardian consent.

On 15 February 2023, Burgos Club de Fútbol terminated the mandatory biometric requirement and introduced an alternative access mechanism based on either fingerprint recognition or identity document verification. At that stage, the AEPD considered that the continued processing of biometric data failed to satisfy the principles of necessity and proportionality and had been carried out without a prior DPIA. Given the risk of serious and irreparable harm to data subjects' rights, the authority imposed a precautionary measure ordering the immediate suspension of the fingerprint recognition system pending the final decision.

On 29 December 2023, the AEPD formally initiated sanctioning proceedings against the club for alleged infringements of Articles 5(1)(c), 8, 9, 13, and 35 GDPR (AEPD, 2024):

(1) The AEPD found a violation of Article 35 GDPR, as the controller had failed to conduct a DPIA before commencing biometric processing. The assessment was carried out only several months later, rendering the initial processing unlawful.

(2) The authority rejected the argument that biometric processing was necessary to comply with obligations imposed by the State Commission. It held that none of the derogations under Article 9(2) GDPR were applicable, and that the mere existence of sectoral security rules could not justify the processing of special category data in the absence of a valid exemption.

(3) Although the controller later relied on data subject consent under Article 9(2)(a) GDPR, the AEPD concluded that no valid consent had been obtained. The only document signed by club members concerned season ticket arrangements and could not be construed as explicit consent for biometric processing.

(4) The AEPD identified a breach of the principle of data minimisation under Article 5(1)(c) GDPR. Also biometric identification was not strictly necessary, as the same security objectives could have been achieved through less intrusive means, notably identity document checks.

(5) The authority found an infringement of Article 8 GDPR, as the system enabled the processing of biometric data of minors without establishing a clearly defined minimum age for unique identification.

(6) The controller failed to comply with Article 13 GDPR, having provided incomplete and insufficient information to data subjects during

In 2024, the AEPD imposed an administrative fine of EUR 200,000 for unlawful biometric processing and violations of the principles of necessity and proportionality. Due to the controller's acknowledgment of responsibility under national procedural law, the fine was reduced by 40% to EUR 120,000 (AEPD, 2024).

Therefore, the AEPD decision in Burgos Club de Fútbol (AEPD, 2024) is of particular relevance as it addresses the interaction between public security considerations, sector-specific regulatory obligations, and the autonomous requirements of the GDPR. The authority unequivocally affirmed that the existence of state-level security measures or recommendations does not, in itself, provide a lawful basis for the processing of biometric data under Article 9 (European Parliament & Council of the European Union, 2016), nor does it exempt controllers from compliance with the principles laid down in Article 5 GDPR. The AEPD explained that biometric identification systems deployed for access control must be assessed against a strict standard of necessity, requiring controllers to demonstrate that the intended purpose cannot reasonably be achieved through less intrusive means. Also, the decision reinforces the preventive function of Article 35 (European Parliament & Council of the European Union, 2016), confirming that the absence of a prior DPIA in high-risk biometric processing operations constitutes an independent and substantive infringement.

The decision reinforces the view that efficiency or convenience (such as faster access through fingerprint recognition) cannot substitute for a rigorous legal assessment of less intrusive alternatives. For controllers, failure to demonstrate such diligence may not only invalidate the processing but also operate as an aggravating factor in the determination of administrative sanctions. The reduction of the fine following the controller's acknowledgment of responsibility under national procedural law does not diminish the normative weight of the findings, which underscore the importance of due diligence, transparency, and ex ante risk assessment in biometric data processing.

The Facial Recognition in SIDEUCU-gym (AEPD, 2025). This part of the research is based on the official documentation and findings of the Spanish Data Protection Agency (Agencia Española de Protección de Datos, AEPD) in the case SIDEUCU S.A. with its decision issued on 26 June 2025.

According to the case facts, SIDEUCU S.A., a company managing several gym centers, implemented a facial recognition system for member access in 5 of its centers starting around July–August 2023. Previously, the gyms used a fingerprint-based access system. The facial recognition system generates a biometric template from the facial image of each member, encrypts it, stores it in the system, and uses it to verify identity upon entry and exit. SIDEUCU S.A. claimed to have placed five informational posters in visible locations at its centers. Each poster, except for the heading indicating the center's name, contained the following general content with the explanation of biometric identification systems, noting that EMPRESA.1 - system extracts facial data points and creates a template using proprietary NIR algorithms with the technical description of how facial templates are created (2D + 3D fusion) and encrypted using AES 256-bit encryption. The posters stated that the system does not store raw images, only encrypted templates, and that the algorithm is proprietary. Claimed advantages, such as fast, reliable identification and prevention of fraudulent use.

Thus, SIDEUCU S.A. is the data controller, as it determines the purposes and means of processing. The software provider (EMPRESA.1) may act as a processor, but the ultimate responsibility rests with SIDEUCU S.A.

Despite the posters, the authority concluded that SIDEUCU S.A. did not comply with GDPR's Article 13 requirements to inform individuals about the processing of their personal data (AEPD, 2025) as follows:

1) There is no documentation showing when the posters were placed, so it is unclear whether they were available before or at the same time the biometric data was first collected, as required by Articles 12 and 13 GDPR.

2) The placement of the posters did not ensure that they were clearly visible and accessible to all members before biometric data collection. Thus, SIDEUCU S.A. was collecting, storing, and using biometric data from facial recognition for access control without properly informing members, constituting a violation of Article 13 GDPR.

3) The posters did not inform members that facial recognition involved processing of special-category personal data - biometric data.

4) Information was based on an incorrect interpretation of manufacturer certificates, without properly evaluation the legal essence of the facial templates generated, stored, and used by EMPRESA.1 software.

The SIDEUCU S.A. claimed that no personal data was being processed, misleading members about the risks involved (AEPD, 2025). Company failed to inform members about all aspects required under Article 13 GDPR (European Parliament & Council of the European Union, 2016), including identity and contact details of the controller and, if applicable, the data protection officer; legal basis and purpose of processing; data recipients; retention period; rights to access, rectification, deletion, restriction, or objection; right to complain to the data protection authority.

The violation characteristics:

(1) Failure to inform members about the processing of special-category data (biometric data), which is considered the high risk. Documentation (registration forms, privacy notices) did not include consent or proper information regarding biometric processing.

(2) Members were forced to use the facial recognition system as the only access method; no alternative methods were provided.

(3) The company acted without due diligence, ignoring warnings from members, and failed to consult experts or official guidelines.

(4) No DPIA was carried out, even though biometric processing is high risk.

(5) Affects the biometric data of members across 5 centres.

(6) Continuous non-compliance during the period biometric data was collected.

An administrative fine of €30,000 was stated, taking into account Article 83 GDPR (European Parliament & Council of the European Union, 2016) criteria (seriousness, intentionality/negligence, type of data, and scope of processing). Also, the authority imposed corrective measures under Article 58(2)(d) GDPR, requiring SIDEUCU S.A. to bring its operations into compliance with Articles 9 and 13 GDPR within a specified timeframe (AEPD, 2025).

Therefore, the facial recognition system constitutes prohibited processing of special category data under Article 9 (1) GDPR. The SIDEUCU case is particularly relevant beyond the fitness sector, as it reflects a growing trend toward the normalization of biometric access control in everyday commercial environments, including

retail, residential buildings, and private services. The decision sends a clear signal that such normalization does not diminish the heightened protection afforded to biometric data under EU law. Even in non-public, low-security environments such as fitness centers, supervisory authorities reaffirm that convenience or efficiency cannot override data protection rulings. The failure to conduct a Data Protection Impact Assessment and to seek expert or supervisory guidance demonstrates a lack of compliance-by-design and compliance-by-default. This governance failure, rather than merely defective information notices, was central to the unlawfulness of the processing. Besides, the AEPD rejected the argument that encryption, the absence of raw image storage, or proprietary algorithmic design neutralizes the legal qualification of biometric data (AEPD, 2025). The legal check should focus more on functional capability, which is unique identification, rather than technical implementation details.

Generalization of the results

The legal examination of biometric access authority under the GDPR must prioritize the functional capacity of the system to uniquely identify individuals, rather than technical design options or formal disparities between identification and authentication. As set in biometric legal doctrine, the assertive factor is whether biometric characteristics are processed for unique recognition, which automatically activates the application of Articles 4(14) and 9 GDPR and an increased legality threshold (Kindt, 2013). Where access to sports or fitness facilities is drilled on biometric enrolment, and no equivalent non-biometric alternatives are offered, consent cannot be considered freely given, mediating a structural power inequality between service providers and users. This assures the consistent GDPR position that consent is invalid when access to essential or contractual services depends on biometric identification.

From a governance standpoint, data-driven technologies and biometric systems in particular must be assessed as rights-affecting infrastructures rather than neutral efficiency tools (Ebers & Sein, 2025). Spanish supervisory enforcement against SIDEKU, S.A., and Burgos Club de Fútbol, S.A.D. operationalizes this practice by rejecting both consent and contractual necessity as lawful bases for biometric access control in sport, thereby confirming a *de facto* presumption of unlawfulness absent unusual rationale.

Ethical analyses further reinforce this legal logic. Biometric identification entails risks of stigma, exclusion, and irreversible misidentification, particularly in everyday social contexts (Smith & Miller, 2021). Spanish supervisory authorities translate these ethical concerns into enforceable legal findings by recognizing that biometric access systems can unjustifiably exclude individuals from socially significant activities such as sport. At the same time, facial recognition technologies function as a democratic stress-test in mass climates, where routine biometric surveillance normalizes bodily monitoring and undermines participatory equality (Menéndez González & Mobilio, 2025).

Ebers and Sein (2025) conceptualize data-driven technologies, including biometric systems, as governance infrastructures that directly shape rights, accountability, and risk management. This perspective is highly relevant to sport, where biometric access control systems embed identity verification into everyday participation. Their framework helps interpret Spanish enforcement practices, showing that biometric deployments in gyms and stadiums are not merely technical tools but rights-sensitive interventions requiring strict oversight, necessity justification, and accountability mechanisms.

Although biometric technologies can, in theory, be produced responsibly and with user-centric safeguards (Salice & Salice, 2024; Vielhauer, 2018), the Spanish enforcement method demonstrates a persistent gap between privacy-by-design ideals and real-world deployments in sport. This gap confirms a broader fundamental-rights insight: biometric data processing marks a boundary of lawful data use, requiring exceptional justification and strict necessity (van der Sloot & Van Schendel, 2024).

Conclusions

This study establishes that biometric data processing systems used for access control, whether based on facial recognition or fingerprint verification, constitute the processing of special categories of personal data under Articles 4(14) and 9 GDPR and whenever its enable or confirm the unique identification of a natural person. The distinction between biometric identification (1:N) and verification/authentication (1:1) does not, in itself, exclude the application of Article 9 GDPR where identification effects are present.

The research shows that generic references to public interest or security objectives are insufficient to justify biometric processing under Article 9(2)(g) GDPR. The Spanish constitutional doctrine and data protection law requirements converge in demanding that any restriction of the fundamental right to data

protection must be established by a law of sufficient normative rank, must indeed define the substantial public interest pursued, and must incorporate precise, foreseeable, and robust safeguards.

The research concludes that Article 13(1) of Law 19/2007 (Spain, 2007) does not meet these requirements and therefore cannot serve as a valid legal basis for mandatory biometric identification in sports venues. Accordingly, national-level regulations imposing biometric access systems without explicit legislative authorization are incompatible with the EU data protection framework.

According to the Article 13(1) of Law 19/2007 (Spain, 2007) - the verification and monitoring of the identity of those who purchase tickets, or the control of seat allocation, shall be carried out through the implementation of personalized ticket sales systems and the development of procedures allowing supervision of seat distribution and identification of the holders of access tickets to sports facilities. The processing of the data obtained through these procedures shall be limited to providing information about those who access or attempt to access sports venues, for the purpose of ensuring compliance with existing prohibitions and, where appropriate, determining any liabilities that may arise.

National law of Spain, particularly, Article 13(1) of Law 19/2007 (Spain, 2007) refers to identity verification systems, but does not contemplate the possibility that such systems may involve the processing of biometric data, nor does it establish the relevant and appropriate safeguards for the protection of the fundamental right to the protection of personal data. Therefore, where the processing of personal data falling within the special categories referred to in Article 9(1) of the GDPR is intended given that these are biometric data aimed at identifying natural persons it is a prior requirement that one of the circumstances set out in Article 9(2) apply to lift the general prohibition on processing established in Article 9(1) (European Parliament & Council of the European Union, 2016). Moreover, the processing operations referred to in point (g) of Article 9(2) of GDPR that are based on Spanish law must be covered by a provision having the rank of law, which may establish additional requirements relating to security and confidentiality.

There is no legal provision authorizing such processing under Article 9(2)(g) of the GDPR (European Parliament & Council of the European Union, 2016), since Article 13(1) (Spain, 2007) does not meet the jurisprudential requirements. Therefore, it concluded that the adoption of an agreement by the State Commission against Violence, Racism, Xenophobia, and Intolerance, within the scope of its powers, establishing compliance measures for clubs consisting of the installation of biometric systems to control access to all entrances to supporters' sections, allowing the unequivocal identification of fans accessing those sections, is not compatible with the data protection regulatory framework.

The examined AEPD prior consultation (AEPD, 2023) and decisions (AEPD, 2024; AEPD, 2025) reveal invariant and strict enforcement of GDPR principles, particularly necessity, proportionality, transparency, and data minimisation. In both the SIDECU and Burgos Club de Fútbol cases, biometric processing was declared unlawful due to the absence of a valid legal basis under Article 9(2) GDPR, the lack of freely given consent, the failure to conduct a prior DPIA, and the availability of less intrusive alternatives.

The study confirms that technical characteristics, such as encryption, proprietary algorithms, or the non-storage of raw images, do not remake the legal qualification of biometric templates as biometric personal data. The decisive criterion is the functional capability of unique identification, not the internal architecture of the system. Organizers shall delete the data of persons who have accessed the sporting event once it has concluded, retaining exclusively the data necessary to identify those who may have engaged in conduct prohibited under Law 19/2007 (Spain, 2007), which may only be disclosed to authorities or bodies competent in matters of public security.

The supervisory authorities reaffirm that convenience, efficiency, or innovation cannot override fundamental rights, and that biometric systems must remain the exception rather than the default in access control practices. Also, important to note, the timing of the consultation, issued in 2022-2023 (AEPD, 2023). As demonstrated by the cases analysed in this study, several companies deployed facial recognition systems in 2024-2025 (AEPD, 2024); AEPD, 2025) without having previously assessed comparable enforcement practice or sought regulatory guidance. SIDECU and Burgos Club de Fútbol had opportunities to avoid the identified infringements and to ensure greater compliance with data protection requirements, including a higher level of regulatory diligence.

REFERENCES

1. Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the concept of personal data (WP 136)*. European Commission. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
2. Article 29 Data Protection Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies (WP 196)*. European Commission. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
3. AEPD (Spanish Data Protection Authority). (2023). *Advisory opinion, Case 0098/2022, Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia (Relevant law: Art. 6(1)(e) & 9(2)(g) GDPR)*. <https://www.aepd.es/documento/2022-0098.pdf>
4. AEPD (Spanish Data Protection Authority). (2024). *Burgos Club de Fútbol, S.A.D.: Complaint upheld under GDPR Articles 5(1)(c), 8, 9, 13 and 35, and Law 39/2015 (Case No. EXP202213792)*. <https://www.aepd.es/documento/ps-00483-2023.pdf>
5. AEPD (Spanish Data Protection Authority). (2025). *SIDECU S.A.: Complaint upheld under GDPR Articles 4(14), 6(1), 9(1), 9(2)(a), 9(2)(g), 13 and 35 (Case No. EXP202313347)*. <https://www.aepd.es/documento/ps-00289-2024.pdf>
6. Bulgakova, D. (2025). Between security and violation of the right to protection of biometric data in the “Burgos” case. In *Human rights and democracy: Proceedings of the scientific and practical conference dedicated to Europe Day* (pp. 17–21). Pravo. https://www.aseu.com.ua/wp-content/uploads/2025/05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D0%9F%D1%80%D0%B0%D0%B2%D0%B0-%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8-%D1%82%D0%B0-%D0%B4%D0%B5%D0%BC%D0%BE%D0%BA%D1%80%D0%B0%D1%82%D1%96%D1%8F_%D0%9A%D0%BE%D0%BC%D0%B0%D1%80%D0%BE%D0%B2%D0%B0_2025.pdf
7. Council of Europe. (2021). *European Convention on Human Rights (as amended by Protocols Nos. 11, 14, 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13, 16)*. https://www.echr.coe.int/documents/d/echr/Convention_ENG
8. Council of Europe. (2021). *Guidelines on facial recognition*. <https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751>
9. Ebers, M., & Sein, K. (Eds.). (2025). *Privacy, data protection and data-driven technologies*. Routledge.
10. European Commission. (2018). *Proposal for a Council decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (COM(2018) 449 final)*. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52018PC0449>
11. European Commission. (2020). *White paper on artificial intelligence: A European approach to excellence and trust (COM(2020) 65 final)*. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf
12. European Data Protection Board. (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Version 2.0)*. https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf
13. European Parliament & Council of the European Union. (1995). Directive 95/46/EC 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*. <https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng>
14. European Parliament & Council of the European Union. (2002). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. *Official Journal of the European Communities, L 201*. <https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng>
15. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
16. Kindt, E. J. (2013). *Privacy and data protection issues of biometric applications: A comparative legal analysis*. Springer Netherlands. <https://doi.org/10.1007/978-94-007-7522-0>
17. Menéndez González, N., & Mobilio, G. (Eds.). (2025). *Next democratic frontiers for facial recognition technology (FRT): The legal, ethical and democratic implications of FRT*. Springer Nature Switzerland. <https://doi.org/10.1007/978-3-031-89794-8>
18. Salice, D., & Salice, J. (2024). *Foundations and opportunities of biometrics: An introduction to technology, applications, and responsibilities*. Apress. <https://doi.org/10.1007/979-8-8688-0509-7>
19. Smith, M., & Miller, S. (2021). *Biometric identification, law and ethics*. Springer International Publishing AG. <https://doi.org/10.1007/978-3-030-90256-8>
20. Spain. (2007). Law 19/2007 of 11 July on combating violence, racism, xenophobia and intolerance in sport. *Boletín Oficial del Estado*, 166, 29946–29964. <https://www.boe.es/buscar/doc.php?id=BOE-A-2007-13408>

21. Spain. (2015). Law 39/2015 of 1 October on the common administrative procedure of public administrations. *Boletín Oficial del Estado*, 236. <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>
22. Spain. (2018). Organic Law 3/2018 of 5 December on the protection of personal data and guarantee of digital rights. *Boletín Oficial del Estado*, 294. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673
23. Spanish Constitutional Court. (2000). *Judgment No. 292/2000 of 30 November 2000*. <https://www.tribunalconstitucional.es/en/jurisprudencia/Paginas/resoluciones-traducidas.aspx>
24. Spanish Constitutional Court. (2019). *Judgment No. 76/2019 of 22 May 2019*. <https://www.tribunalconstitucional.es/en/jurisprudencia/Paginas/resoluciones-traducidas.aspx>
25. van der Sloot, B., & Van Schendel, S. (2024). *The boundaries of data*. Amsterdam University Press. <https://doi.org/10.1515/9789048557998>
26. Vielhauer, C. (Ed.). (2018). *User-centric privacy and security in biometrics*. The Institution of Engineering and Technology.