THE PRINCIPLE OF PROPORTIONALITY AND THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION : THE BIOMETRIC DATA PROCESSING

Antonio TRONCOSO REIGADA[1]

Lex Electronica, vol. 17.2 (Automne/Fall 2012)

Table of contents

---

[1] Antonio Troncoso Reigada. Director of the Data Protection Agency of the Region of Madrid 2001-2010, appointed unanimously by all political and trade union groups of the Region of Madrid. He is author of the book *La protección de datos personales. En busca del equilibrio,* Tirant lo blanch, Valencia, 2010. He is a Professor of Constitutional Law; PhD in Law in Bolonia University (summa cum laude). He was honoured with the "Nicolás Pérez Serrano Award" for the best doctoral thesis of Public Law. First National Award for finishing his college studies. He has been the Director General of Services Quality and of the Institute for Statistics of the Region of Madrid, in the Ruiz Gallardón Government. He has been Director of the Technical Office of the Subsecretary of the Spanish Ministry of Health and Consumer Affairs.

I. The limits to the fundamental right to personal data protection in Europe.

The fundamental rights of individuals are not absolute rights, but are subject to restrictions. Hence, the fundamental right to privacy and personal data protection is also subject to restrictions[2]. Obviously not all restrictions on the fundamental rights of individuals are legitimate or justified, and any restrictions imposed have to meet certain requirements. In general, restrictions on fundamental rights are legitimate when they are imposed to protect other constitutional rights, are provided for by law and comply with the principle of proportionality.

The European Court of Human Rights (ECHR) has included the right to personal data protection in Article 8 of the European Convention on Human Rights (ECHR) which protects the right to privacy. The rights recognised in Article 8 of the ECHR are not absolute rights, and may be subject to restrictions or interference by a public authority. The same article that recognises the right to privacy sets out the limits thereto and establishes the conditions of restrictions on the rights recognised in Article 8, as well as the right to privacy and personal data protection. Accordingly, Article 8.2 stipulates that *"[t]here shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest 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*". Accordingly, the ECHR sets out three requirements for justifying interference with a fundamental right: it must be provided for by law; considered to be necessary in the interest of national security, public safety, economic well-being, for the prevention of disorder or crime, for the protection of health or morals and the rights and freedoms of others, and for the maintenance of a democratic society. If these requirements are not met, interference is not justified and is a violation of the fundamental right to personal data protection.

---

[2] In 1873, Judge Cooley, in his book *The Elements of Torts*, defined the right to privacy as "the right to be alone". The formulation of the right of privacy is first used in an article published in 1890 in the *Harvard Law Review* by SAMUEL D. WARREN and LOUIS D. BRAUDEIS under the title: "The right of privacy". Cfr. L. TRIBE, *American Constitutional Law*, 3º ed, The Foundation Press, Mineola, New York, 2000, p. 1338-1345; R. H. BORK, *The tempting of America. The Political Seduction of the Law,* New York, Touchstone, 1990, p. 96-100; G. GUNTHER y K. M. SULLIVAN, *Constitutional Law,* 13º ed., Foundation Press, 1997, 527-530 y 1107-1110; W. F. MURPHY, J. E. FLEMING y W. F. HARRIS, *American Constitutional Interpretation,* Foundation Press, New York, 1986, pp. 106-125, 891-892, 899 y 1081-1092.

The Court of Justice of the European Communities (CJEC) has also recognised the fundamental right to personal data protection. CJEC case law considers that restrictions may only be imposed on the exercise of those rights, provided they effectively meet objectives of general interest pursued by the Community and do not constitute, as regards the aim pursued, a disproportionate and intolerable interference, impairing the very substance of those rights. Article 52 of the Charter of Fundamental Rights of the European Union - which recognises in the Article 8 the fundamental right to personal data protection- contains a general clause setting out the scope of guaranteed rights. Hence, while the ECHR does not recognise the right to privacy as an absolute right and expressly establishes limits thereto, the Charter recognises the rights in an absolute manner and contains a clause of limitation in Article 52.1 which stipulates that *"[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*". Nevertheless, the Charter does not aim to decrease the level of protection of the rights provided for in the Convention, and there is therefore no justification for curbing the rights that are not subject to restrictions in the ECHR or have fewer restrictions than those provided for in the Charter. Article 52.3 of the Charter stipulates that *"[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection*".

Nor does Community Directive 95/46/EC on the protection of individuals with regard to the processing of personal data define it as an absolute right, setting limits thereto. The European Commission has adopted a Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) -which will repeal the actual Directive 95/46/EC and and displace the laws of the Member States- that also contains limits to the fundamental right to personal data protection[3]. The case law of the Spanish Constitutional Court

[3] COM (2012) 11 final y COM (2012) 10 final, 25.1.2012. The European Commission has argued different reasons to promote the adoption of this new European regulatory framework: the adoption of the Lisbon Treaty, the profound

acknowledges that the public authorities may restrict fundamental rights, including, therefore, the fundamental right to personal data protection. It has, however, established a specific constitutional rule that requires compliance with certain criteria for restrictions to be considered legitimate: the restriction must be adequately provided for by law and clearly understood by the citizen; it has to serve a legitimate purpose; and its implementation must be justified and proportional[4]. The case-law of the Constitutional Court has used two instruments to strike a balance between rights and their limitations: the essential content of those rights and freedoms, which is a general and abstract safeguard for the protection of fundamental rights, and the principle of proportionality. Pursuant to Spanish constitutional case law, therefore, the restriction of the right to personal data protection must be provided for by law, be imposed to protect other constitutional rights, and comply with the principle of proportionality. Logically, if the restriction violates the essence –the essential content, the essential core- of those rights, it is a violation of the principle of proportionality.

1.1 The accessibility and predictability rule

The first requirement for the restriction of the fundamental right to personal data protection is that it must have a legal basis. This requirement can be found in the ECHR, the Constitutions of the Member States, the case law of the ECHR and the Constitutional Courts of the Member States[5]. The ECHR has not interpreted the requirement of legal provisions as a legal requirement in the formal sense, but in the material sense, and points to what the different legal systems have defined as a law[6]. In any event, the ECHR requires that the law meet two requirements: accessibility and predictability[7]. Accordingly, in its Ruling of 26 April 1979, on the *Sunday Times Case*, and in

changes that ICTs have experienced in recent years with the arrival of the Internet and social networking and the differences in the protection of personal data among different Member States which impede the internal market and the exercise of this fundamental right. The text of the proposed regulation introduces main changes with regard to the territorial scope, general obligations of the controller, the strengthening of the supervisory authorities, the principles and rights, making special mention of the right to be forgotten in the online environment.

[4] As pointed out in Constitutional Court Ruling 169/2001, "the proportionality of measures restricting fundamental rights constitutionally requires, moreover, legal provisions there for and proof that it is a suitable, necessary and proportionate measure in relation to the constitutionally legitimate end". See also Constitutional Court Ruling 134/1999.

[5] In Ruling 207/1996, of 16 December, the Constitutional Court ruled that "the restriction of this right (the right to privacy) may only be imposed in accordance with a mandatory legal provision".

[6] Accordingly, for example, the concept of law in the formal sense does not exist in Community law.

[7] On this matter, see the Ruling of the ECHR of 25 March 1993, on the "Costello-Roberts/UK Case" and the Decisions of the ECHR, nos. 8239/1978 y 8278/1978

relation to the expression "provided for by law", the ECHR ruled that the first condition "*means that the law has to be sufficiently accessible, that is to say, the citizen has to have sufficient information on the legal rules applying to the case; the second condition means that a rule cannot be considered a law unless it is worded with sufficient precision to enable the citizen to adapt his conduct accordingly; he must be able to foresee the consequences of a particular action from the explanations provided*". In Ruling 292/2000, of 30 November, F. J. 9º, the Spanish Constitutional Court also stressed the importance of accessibility and predictability, stating that "*the law establishing the limits must be accessible to the individual concerned, he must be able to foresee the consequences of its application, the restriction must be imposed in response to a vital social need, and it must be adequate and proportional to the achievement of that objective*".

The condition of "predictability", that is to say, that the law is sufficiently clear and detailed to ensure that the citizen has sufficient information on the measures that may be taken in the event of non-compliance and can adapt his conduct accordingly, is particularly important for justifying the restriction on the fundamental right to personal data protection. Nevertheless, one must be aware that a law cannot regulate every single case justifying the restriction of this fundamental right. Accordingly, a law does not violate the condition of predictability when it allows the exercise of discretional power, provided it sets out the scope thereof and the means of exercising it sufficiently clearly, and also stipulates the instruments of control. In the *Malone Case* of 2 August 1984, therefore, the ECHR states that the law must clearly indicate the level of discretion of the public authorities and its purpose so that the citizen has sufficient knowledge to react to the arbitrary action. In the *Kruslin and Huvig Cases* of 24 April 1990, the ECHR states that the processing of personal data is a violation of the right set out in Article 8 of the ECHR when it fails to provide for the necessary safeguards. The ECHR states that for a legal rule that limits data protection rights to meet the condition of predictability, it has to be clear and concise and indicate the legitimate circumstances in which data may be processed, the procedure that will be followed; the information that will be collected and stored, indicating, in the latter case, the duration and conditions thereof; the procedure for accessing and disclosing personal data, the authorities that have access thereto and to whom the data may be disclosed; in addition to the procedure for notifying, rectifying and cancelling the data collected. Accordingly, in the *Rotaru Case* of 4 May 2000, the ECHR ruled that

the absence of a procedure to protect the rights of the individual concerned and to control the activity of the Administration was a violation of data protection legislation.

1.2 The legitimate purpose. The preference of freedom of information over the protection of personal data.

The second requirement for the restriction of the fundamental right to personal data protection is that it serves a legitimate purpose or protects a constitutional right. Article 8.2 of the ECHR sets out the circumstances in which interference with the right to privacy is justified: national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and for the protection of the rights and freedoms of others. Fulfilment of the legitimate purpose requirement has not represented a serious obstacle for the ECHR as, up until now, it has limited its involvement to determining whether one of the aforementioned legitimate purposes applied. Accordingly, the processing of personal data without the consent and knowledge of the data subject is justified when it is in the interest of national security, public safety, the prevention of disorder and crime, and, in particular, terrorism. The ECHR understands that states have ample room for manoeuvre and that the decision as to whether the interference is justified in the interest of one of the aforementioned legitimate circumstances is left to the national authorities.

The data protection regulation, Convention 108, the Community Directive –also the Proposal for a General Data Protection Regulation 2012- and national legislation have established legislative measures to restrict the scope of data protection obligations and rights when such a restriction constitutes a necessary measure to safeguard national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences; an important economic or financial interest and the protection of the data subject or of the rights and freedoms of others[8]. Furthermore, Directive 95/46/EC and national legislation allow the processing of specially protected data without the data subject's consent for health care purposes.

[8] Furthermore, the Directive allows the restriction of the rights of access, correction, cancellation and opposition when the data is processed solely for statistical or scientific purposes.

In contrast to Convention 108, Directive 95/46/EC –also the Proposal for a General Data Protection Regulation 2012- lists the circumstances in which the processing of personal data without the data subject's consent is legitimate. Accordingly, Section II of the Directive –art. 6 of the Proposal for a General Data Protection Regulation 2012-, entitled "Criteria for making data processing legitimate", states in Article 7 that Member States shall provide that personal data may be processed only if, in addition to when the data subject has unambiguously given his consent, "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 7 (b)); is necessary for compliance with a legal obligation to which the controller is subject (Article 7 (c)); is necessary in order to protect the vital interests of the data subject (Article 7 (d)); is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (Article 7 (e)); or for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) of the Directive ((Article 7 (f))[9]. The first two conditions may be understood as tacit consent; the third is a manifestation of the priority given to life and health, which we already referred to. The last two conditions, tasks carried out in the public interest and for the purposes of the legitimate interests of third parties, are worth a special mention as they are a restriction of consent and, therefore, of the fundamental right to personal data protection.

Most Member States have transposed the condition relating to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed into national law exactly as set out in Article 7 (e) of the Directive – art. 6.1.e) Proposal for a General Data Protection Regulation 2012-, without providing further clarification. As stipulated in Recital 32 of the Directive, it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association. Most Member States allow the processing of personal data without the data subject's consent when this is necessary for the

[9] See Articles 6 and 11 of the LOPD and Article 5 of Regulation 45/2001/EC.

performance of a task carried out in the public interest or in the exercise of official authority without requiring that law establish this administrative function. Other Member States have been more restrictive, only allowing data to be processed when the function in question is established by law or a regulation enacted by virtue of a law, and sets out the corresponding tasks and functions[10]. Nevertheless, most Member State Administrations are bound by the principle of legality, which means that the Public Administrations may only act when so empowered by law and with ample regulatory collaboration. The Spanish Data Protection Law (the LOPD) allows personal data to be processed without the data subject's consent "for the performance of the functions of the Public Administrations within the scope of their powers" without there being any specific legal provision there for. The LOPD also allows the transfer of data between Public Administrations in the exercise of different powers or of powers relating to different matters "when such transfers are provided for in the file provisions or by a higher provision regulating the use thereof". Nevertheless, this section was declared unconstitutional by the Spanish Constitutional Court Ruling 292/2000 of 30 November, and it is thus required that a law exist to provide for such transfers, unless the data transfer relates to common competencies or powers or competencies relating to the same matters[11]. It is one thing that the Public Administration always act in accordance with the law, bound, thus, by the principle of legality, and quite another that the law provide for the transfer of data. This is not required by the Community Directive, nor is it a requirement of the essential content of the fundamental right. In our opinion, it is appropriate that the transfer of personal data among the Public Administrations be provided for by a regulation implementing rules for the law. The requirement that a law always exist means that many legal powers are no more than general rules.

The LOPD does not expressly refer to "the performance of a task carried out in the public interest", and, as pointed out previously, uses the expression "for the performance of the functions of the Public Administrations within the scope of their powers or competencies". The only time the LOPD cites public interest is in the exception to the rights to access, correction and cancellation when "*after considering the interests at stake, the rights granted to the data subject by virtue of these*

---

[10] See the Analysis and impact study on the implementation of Directive EC 95/46 in Member Status. We must specifie as an exception the case of Latvia and Portugal, where the task carried out in the public interest must be expressly provided for by law.

[11] A review of this Constitutional Court Ruling can be found in A. TRONCOSO REIGADA, "La protección de datos personales. Reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público,* 2003, núms. 19-20, 2003, pp. 231-334.

rules must be overridden for reasons of public interest or third-party interests that are in greater need of protection"[12]. Nevertheless, this rule was declared unconstitutional by Ruling 292/2000, which considers that the use of "public interest" to justify the restriction of a fundamental right of Article 18.1 and 4 of the Spanish Constitution is far too ambiguous. Accordingly, all administrative activity is ultimately aimed at serving general interests objectively (Article 103.1 of the Spanish Constitution) and may be used to justify the processing of personal data without the data subject's consent, but not the exception of the rights to access, correction and cancellation.

Article 7 (f) of the Directive - art. 6.1.f) of the Proposal for a General Data Protection Regulation 2012- sets out as legitimating principle of treatment if it "is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". This "balance" criterion has been transposed into national law in terms identical or close to those used in the Directive. According to a report commissioned by the Commission, Member States must take into consideration the nature of the data; the nature of the processing; whether the processing is carried out in the private sector or the public sector; and the measures which the controller has taken to protect the interests of the data subject. It is noteworthy that the Member States exercise greater control when it is the controller of a public file that makes use of this criterion for the legitimacy of data processing. The Member States have generally implemented this provision in a more restrictive manner than it appears in the Directive and subject it to additional requirements. In general, the balance of interests is tilted towards the data subject, or limits its application to certain narrowly defined data, or to cases specified by the Data Protection Authority. There are substantial divergences between Member States on this matter. In Germany, for instance, somewhat differently phrased tests are applied to the private sector and the public sector, respectively [13].

[12] The LOPD cites public interest when it authorises the transfer of data to other countries that do not have the same level of protection, provided "it is necessary or legally required for the protection of a public interest. The transfer requested by a tax or customs authority in the exercise of its powers shall have such a consideration".

[13] In Finland, the law sets out a limited number of cases in which data can be processed and which can be seen as special applications of the "balance" test, but otherwise requires controllers who believe they can rely on this test to obtain a permit from the Data Protection Authority.

The absence of this provision in the LOPD is justified by the government, in the sense that the legislator sets out those specific cases where the balance test authorises controllers to carry out the processing of personal data without the data subject's consent. Consequently, such processing operations would be those necessary for credit reporting purposes, insurance purposes (e.g. aimed at identifying fraud) and any operations involving the processing of certain type of data which would be made publicly available from the so-called publicly available sources, such as the promotional census, the telephone directories, official journals, etc. Nevertheless, let us not forget that Recital 30 of the Directive cites as reasons for Article 7 (f) "*to maintain a balance between the interests involved, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies and for the purposes of marketing*". In the Commission's opinion, Spanish Law is still restrictive on this point, as pointed out in the report commissioned by the Commission[14]. Recently, the Court of Justice of the EU, in the judgment of 24.9.2011, stated the incorrect transposition of the Directive by the Spanish legislation.

The Article 8 of the Directive -art. 9 of the Proposal for a General Data Protection Regulation 2012- allows the processing of "special categories of data" where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (Article 8.1). Member States may also lay down exemptions either by national law or by decision of the supervisory authority for reasons of substantial public interest (Article 8.4). The derogations from the prohibition to process special categories of data shall be notified to the Commission (Article 8.6). Nevertheless, as the report commissioned by the Commission points out, provisions adopted on the basis of Article 8 (4) are only very rarely notified to the Commission by Member States and the Commission therefore has an incomplete understanding of the implementation of Article 8 (4). From this the Commission gathers that the laws in the Member States provide for few specific exemptions

[14] This peculiarity together with the fact that the Spanish law confers a special treatment to processing that consists of disclosure of information to a third party ("cesion de datos") makes the processing of personal data without consent of individuals considerably more difficult in Spain than in other countries. See the Analysis and impact study on the implementation of Directive EC 95/46 in Member States.

to the in-principle prohibition on the processing of sensitive data, on the lines envisaged by Article 8 (4), although several of them allow for the adoption of subsidiary rules of this kind or the issuing of ad hoc authorisations. France and the UK have only issued such authorisations until now.

As pointed out earlier, Article 13 of the Directive, entitled *Exemptions and restrictions*, -art. 21 of the Proposal for a General Data Protection Regulation 2012- allows Member States to adopt legislative measures to restrict the scope of the obligations and rights "*when such a restriction constitutes a necessary measure to safeguard national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority; the protection of the data subject or of the rights and freedoms of others*"[15]. According to the Commission's report, such restrictions may take account, for example, of the need to fight crime or to protect public health in emergencies[16]. Other provisions of the Directive contain a similar possibility for limited exceptions, such as the previously mentioned protection of an important public interest. This mechanism, open to Member States' appreciation of what may constitute "a necessary measure" and an "important public interest", is a major source of discrepancy among national legislations.

The Community Directive has also introduced an important restriction of the fundamental right to personal data protection in favour of freedom of expression and information when the processing of personal data is carried out solely for journalistic purposes or the purpose of artistic or literary expression and to protect intellectual property and copyrights –see also art. 80 of the Proposal for a General Data Protection Regulation 2012-. Freedom of information has historically been considered an important freedom, a *primus inter pares*, as it is essential for the freedom of public opinion required in a democratic society, and to limit power. Indeed the control of information has always been a priority for those in power and a characteristic of authoritarian regimes. Nowadays,

[15] The European Union has concluded an International Agreement with the US to address the use of passengers' PNR data to fight crime. See Court of Justice of the EU, judgment 30.6.2006, as. *PNR*, (C-317/04 y C-318/04-.
[16] See the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Brussels, 7.3.2007, COM (2007) 87

democratic states aim to further increase administrative transparency and the flow of information on matters of public interest. It is the importance of freedom of information that justifies the restriction of the right to personal data protection and has thus been expressly provided for in the Directive and in the Proposal for a General Data Protection Regulation 2012.

Consequently, Recitals 17 and 37 of the Directive set out that the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing. The Directive stipulates that the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities. Accordingly, Article 9 of the Directive concerning the Processing of personal data and freedom of expression stipulates that "*Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*". This does not mean that the media is entirely exempt from data protection legislation, but that the necessary restrictions must be introduced only if it is necessary to facilitate freedom of information and expression. Consequently, consent of the data subject for the processing of personal information, including audiovisual data, cannot be required of a media organisation when such activity clearly serves a public interest. The exceptions provided for in Member State legislation may affect, for example, data transfers to third countries and the powers of the supervisory authorities[17], but not the regulations governing data processing security. Therefore, it does not make sense that an administrative authority, such as the Data Protection Agency, is

[17] The restriction must be imposed by the judicial authority. Nevertheless, because this requirement is not set out in Article 18.1 of the Spanish Constitution, it may also be imposed by the administrative authorities, provided they are legally empowered thereto.

empowered to restrict the exercise of a fundamental right like freedom of information, which is so important for a democratic society.

This, in the Commission's opinion, is the area where "least convergence can be discerned"[18]. Consequently, for example, Spanish law makes no reference to the processing of personal data for the exercise of the right to freedom of information and expression, but merely sets out the provisions for the publication of personal information by the social media that is considered accessible to the public[19]. Nevertheless, the fact that Spanish Data Protection legislation does not mention the processing of personal data by the media does not mean that such processing is excluded from the scope of the legislation[20]. It should be pointed out that Spain has no specific law to regulate the freedom of information and expression. The absence of such a law is no coincidence, but a conscious decision to not restrict the exercise of this fundamental right excessively, leaving the definition of the limits thereof to the Constitutional Court. Nevertheless, it is logical that the right to personal data protection is restricted by the right to freedom of information. This is not unusual for the Spanish legal system, as, pursuant to the Constitution, the right to information overrides the right to privacy (Article 20.1.d)[21].

It should also be pointed out that freedom of information is not an absolute right and it cannot, therefore, eliminate the right to privacy and personal data protection, which are necessary for the dignity of the individual and the quality of human life[22]. Furthermore, without denying the social function of freedom of information, it must be pointed out that the fundamental right to personal data protection, and the right to privacy, should not be perceived, as in *iusprivatista dogma*, as an individual right like the right to property, which only affects the parties concerned, but as an essential and objective element that affects all of society. There is a public interest in respect for the

---

[18] See the Analysis and impact study on the implementation of Directive EC 95/46 in Member States, *loc. cit*.
[19] See Articles 3 j) and 28.3 of the LOPD.
[20] Indeed such processing is not excluded from the scope of the LOPD, nor is it remitted to the specific legislation – article 2 of the LOPD-.
[21] Although the fundamental right to personal data protection is overridden by the right to information, this does not seem to be the case with the freedom of expression provided for in Article 20.1.a). Nevertheless, the spread of Internet access, blogs and interactive websites means that the right to freedom of information is no longer restricted to certain professionals, and that everyone has the ability to obtain information and that this information is accessible to all of society.
[22] Accordingly, Spanish Constitutional Court Ruling 57/1994 recognises it as a right that is "strictly linked to the personality itself and contributes to the dignity of the individual (…) the constitution protects privacy and recognises the existence of personal space that is protected from the activity and knowledge of others, necessary, according to the norms of our culture, for maintaining the quality of human life".

right to privacy and personal data protection. While the direct beneficiary of privacy and personal data protection is the data subject himself, it indirectly benefits all of society, as the exercise of the rights and freedoms -the right to decision-making and independence- implies control over one's personal information. For this reason, the exercise of the right to freedom of information must comply with the principles and rights to personal data protection.

Logically, freedom of information is not an absolute right, and it has to respect the individual's right to privacy and personal data protection. Our constitutional case law has established a set of criteria that is useful for distinguishing between freedom of information and the right to privacy, as well as the protection of personal data[23]. If freedom of information is to prevail, the personal information processed or disseminated by the media must be of public interest, that is to say, of a newsworthy nature, either because of the object, when its content is of a collective or general interest, or because of the subject, when the data subject is an important public figure. A matter is of importance to the public when knowledge thereof is of general interest because it refers to a socially controversial matter or event that affects citizens in general, as opposed to a few private individuals. Some people, because of their profession or public position, are in the public eye and are therefore more subject to the criticism and scrutiny of the public than unknown individuals. Likewise, certain matters of public interest may be disseminated and, in this case, the collection and processing of personal data may be justified, even when this affects the privacy of the individual and restricts his or her right to control information about himself. Such an individual may not object to the media processing or publishing this information, even when it relates to the private domain[24]. The priority of freedom of information over the protection of personal data is also a logical consequence of ideological freedom, of political plurality and, in short, the principle of democracy[25]. Nevertheless, freedom of information also has its limits. People of public interest, because of their profession or the position they hold, maintain the right to privacy. One of the conditions of the freedom of information is that it is truthful, which, according to the Constitutional Court (Ruling 6/1988), means that the information is diligently obtained and in good faith. Consequently, personal data processing by the media must always comply with the principle of quality, which, in this case, means that the

[23] See M. CARRILLO, *El Derecho a no ser Molestado. Información y vida privada*, Thomsom, Aranzadi, 2003, p. 25-37.
[24] As we have mentioned on other occasions, the fundamental right to data protection does not only protect private information, but all types of data, private or otherwise. See A. TRONCOSO REIGADA, *loc. cit.* p. 244-252.
[25] See J. H. ELY, *Democracy and distrust,* Harvard University Press, 1980; M. ARAGÓN, *Constitución y democracia,* Tecnos, Madrid, 1990.

information processed is truthful and accurate. Moreover, the fact that the information is truthful is not sufficient justification for processing and disseminating it. The dissemination thereof must be in response to a public interest, as pointed out previously.

Another important restriction on the fundamental right to data protection established by the Directive –and by the Proposal for a General Data Protection Regulation 2012- is the protection of intellectual property and copyrights. Accordingly, while all persons must be able to exercise the right of access to data relating to him which are being processed and know the logic involved in the automatic processing of data concerning him, Recital 41 of the Directive stipulates that "*this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software*" whereas these considerations must not, however, result in the data subject being refused all information[26].

In contrast to the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter of Fundamental Rights of the European Union does not specify the purposes that justify the restriction of a fundamental right, but merely states that any limitations thereto must be necessary and respond to general interests recognised by the European Union or to protect the rights and freedoms of others. This has been the stance adopted by the European Constitutional Courts. In the famous ruling on the Census Act, the German Federal Constitutional Court recognised the existence of the right to information self-determination within the general rights to human dignity and personality -article 2.1 *GG,* in relation to Article 1.1 *GG*-. This Judgment stipulates that "*the individual does not have an absolute, limitless right to his personal data; the individual is no more than a personality that moves in a social community. The information, even when personal, represents an aspect of the social reality and does not ultimately depend on the wish of the individual. […] The individual must therefore accept that there are restrictions on the right to information self-determination due to general interests*". The German Constitutional Court has

[26] This is one reason for refusing the right to access personal data in the USA.

therefore subjected the legitimacy of personal data processing by the public authorities to the purpose for which the data will be used[27].

1.3 The principle of proportionality.

The third requirement of any limitation on the exercise of a fundamental right, and, therefore, the fundamental right to personal data protection, is compliance with the principle of proportionality. This principle entails the carrying out of several assessments that values together the limitation of the fundamental right, i.e., interference with the right to personal data protection and the objective pursued, i.e., the legitimate aim analyzed before. The principle of proportionality is provided for by European Public Law, particularly German Law, and has been embraced by Community Law and the case law of the Spanish Constitutional Court as a principle that can be sub-divided into three sub-principles: appropriateness, necessity and proportionality in the strict sense[28]. Accordingly, in order to ascertain whether interference exceeds the principle of proportionality, it must undergo three tests: assessments of its appropriateness, necessity and proportionality in the strict sense[29].

The principle of appropriateness requires that the measure, that is to say, the restriction on the fundamental right to personal data protection, is likely to achieve the proposed objective. It therefore involves an assessment of its appropriateness to ascertain whether the means justifies the end. If interference with the fundamental right to personal data protection does not achieve the proposed objective, it is understood that it is a disproportionate restriction.

---

[27] See in Germany, see K. VOGELSANG, *Grundrechte auf informationelle Selbtsbestimmung*, Baden-Baden, 1987; there is a descriptive overview in T. MAUNZ and R. ZIPPELIUS, *Deutsches Staatsrecht*, 29th ed, C.H. Beck, München, 1994, p. 167-168; and H. HORSTKOTTE, *La protección de datos en Alemania*. Internationes, Bonn, 2001.

[28] See M. MEDINA GUERRERO, "*El principio de proporcionalidad*", *Cuadernos de Derecho Público*, no. 5, 1998 and M. GONZÁLEZ BEILFUSS, *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*, Aranzadi, Pamplona, 2003.

[29] As pointed out in Constitutional Court Ruling 207/1996, "when assessing whether the restriction of a fundamental right exceeds the principle of proportionality, it is necessary to ascertain whether it meets the following three requirements or conditions: whether the measure in question is likely to achieve the proposed objective (the principle of appropriateness); whether, in addition, it is necessary because there is no less extreme measure that can achieve the same objective with the same level of effectiveness (principle of necessity); and finally, whether it is weighted or balanced in that it results in more benefits and advantages to general interest than damage to conflicting goods or values (the principle of proportionality in the strict sense)".

The principle of necessity requires that the measure, that is to say, the restriction on the fundamental right to personal data protection, is necessary to achieve the proposed objective. It is necessary when no less extreme measure can be taken to achieve the objective. It is always necessary to look for the most moderate measure that is capable of achieving the same objective with the same level of effectiveness. When other measures can be taken to achieve the same objective, the least restrictive of fundamental rights shall be adopted. Accordingly, an assessment of the need to interfere with the fundamental right to personal data protection is conducted. If the fundamental right to personal data protection is restricted when other measures that are less harmful to this right can be adopted to achieve the same objective, it is understood that the limitation is disproportionate because it is not necessary –it does not pass the necessity test-.

The principle of proportionality in the strict sense requires that the measure, that is to say, the restriction of the fundamental right to personal data protection, is proportionate to the proposed objective, taking into consideration the nature of the harmed right, the intensity of the interference and the constitutional value it aims to achieve. It is not enough that the limitation on the right to personal data protection is appropriate to achieve the objective and is necessary because no other, less extreme measure can be taken to achieve the same purpose. The measure adopted, i.e., the interference with the fundamental right to personal data protection, must also be proportionate to the objective pursued. It is about reaching an acceptable compromise between two constitutional values: the fundamental right to personal data protection, which will be restricted, and the constitutional value that the processing of personal data is aiming to achieve. Logically, the two constitutional values should be of similar importance. An assessment, or a cost-benefit analysis of the two fundamental rights is conducted to ascertain whether the cost of limiting the fundamental right to personal data protection is proportionate to the legitimate purpose, or benefit it is aiming to achieve. Interference is in compliance with the principle of proportionality in the strict sense when the measure is balanced and results in more benefits and advantages to general interest than harm to other conflicting values. It is understood that the measure fails the proportionality test if the objective pursued is less important than the restriction of the right to personal data protection.

Therefore, the principle of proportionality in the strict sense entails an assessment of the restriction of the right to personal data protection and the constitutional value it aims to achieve, to ensure that

the effort required to achieve the objective is not excessive or disproportionate. To ascertain whether interference is disproportionate, it is necessary to consider how the fundamental right will be restricted, for instance, the restriction imposed on the right to information, consent, access and cancellation of the data, etc.; the type of data that will be processed, whether the processing involves specially protected data; and the safeguards in place to ensure that the fundamental right is protected. It must also be considered whether the objective pursued is an important constitutional value. Finally, the individual interest of the person whose fundamental right is affected should be considered, as well as the existence or absence of a general interest.

The principle of proportionality has been expressed in different ways in the wording of the different regulations. The ECHR stipulates that interference with the exercise of the right must be "necessary in a democratic society". Indeed all of the articles of the ECHR that provide for the restriction of a right require that such a measure is "necessary in a democratic society". Accordingly, the ECHR considers that for interference to be justified, it is not enough that it pursues a legitimate purpose, such as national security and public order, and that this is provided for by law. There must, moreover, be serious reason to justify that interference is "*necessary in a democratic society". The principle of proportionality is used to ascertain whether interference is indeed "necessary in a democratic society*". This principle, while not expressly set out in any of the provisions of the ECHR, has been used by the ECHR, albeit with a different approach. The ECHR does not sub-divide the principle of proportionality into three sub-principles, but assesses it at two points in time: firstly, it determines the need for the measure in a democratic society, which would be equivalent to the sub-principles of necessity and appropriateness; and secondly, it takes into account the proportionality of the measure in the strict sense by weighing up the means used and the objective pursued, which would be the equivalent of the principle of proportionality in the strict sense. In the ECHR's opinion, a measure is *necessary* when there is "*a pressing social demand*" therefore. There must be a fair, pertinent and sufficient reason for a state to impose a restriction on a fundamental right. If there is no sufficient reason therefore, the measure shall not be necessary or justified. Secondly, the measure must be necessary *in a democratic society,* which means that it must be necessary in accordance with the level of shared European values where fundamental rights are guaranteed. Consequently, to ascertain whether interference is justified, the ECHR checks whether the measure taken by the public authority is "necessary in a democratic society". Using the principle

of proportionality, it checks whether there is a *pressing social demand* therefore, and, above all, whether the measure taken is proportionate, in the strict sense, to the legitimate objective pursued[30].

II. The search for balance. A case of limitation of the fundamental right to personal data protection: the processing of biometric data and the principle of proportionality.

This theoretical approach to the restriction of the fundamental right to data protection and the principle of proportionality should be taken into account when ascertaining the legitimacy of the processing of certain types of personal data which interfere with the fundamental right to personal data protection. Indeed many disputes over the restriction of the right to personal and family privacy and physical integrity have been settled using the principle of proportionality[31]. One practical

[30] Strasbourg Court understands that the Member States have a certain margin of appreciation, but the ultimate decision as to whether a restriction is compatible with the European Convention for the Protection of Human Rights is left to the Court. Accordingly, in the *Silver Case* (1983), the ECHR summarised the principles arising from the requirement of "democratic necessity". The Strasbourg Court understands that the phrase "necessary in a democratic society" means that interference is only justified in response to an "urgent social need" or "*a pressing social demand*" and that it must be proportionate to the pursued objective. It maintained that the expression "necessary" was not a synonym of "indispensable", nor did it have the same flexibility as the expressions "admissible", "ordinary", "useful", "reasonable" or "desirable. Moreover, it pointed out that the articles of the European Convention that provided for restrictions on fundamental rights were to be interpreted in a restrictive manner.

[31] Accordingly, in a case of bodily privacy, the Spanish Constitutional Court understood that cutting the hair and shaving the armpits of a suspect in a lawsuit concerning offences against public health did not pass the proportionality test and that the individual's right to physical integrity had been harmed (Constitutional Court Ruling 207/1996). In Constitutional Court Ruling 98/2000 (*Microphones at La Toja Casino Case*), the Constitutional Court understood that the recording of all of an employee's conversations during the working day was not proportional to the pursued objective, that is to say, to guarantee security, as it did not respect the minimum possible sacrifice criteria of fundamental rights. On the other hand, in Constitutional Court Ruling 186/2000, the Court understood that the installation of cameras at the cash registers of the storeroom of ENSIDESA was a proportional measure, considering the irregularities detected there. It was considered an appropriate, necessary and balanced measure because it was restricted to a specific area of the company and for a limited time period. The same principle of proportionality must be applied to the control of e-mail in the workplace. The Spanish Constitutional Court has pointed out that any measure that restricts the individual's right to privacy and physical integrity in criminal law must comply with the principle of proportionality (Constitutional Court Rulings 37/1989, 85/1994 and 54/1996). Likewise, as indicated in Constitutional Court Ruling 207/1996, "a common and constant requirement for the constitutionality of any measure restricting a fundamental right, including interference with the right to physical integrity and privacy, and, most especially, the measures restricting fundamental rights adopted in the course of criminal proceedings, are determined in strict compliance with the principle of proportionality". The need to comply with the principle of proportionality in the collection of DNA samples was

example of the use of the principle of proportionality is to be found in the evaluation of the legitimacy of the processing of biometric data, which is the case of the digital fingerprint. Biometric data is processed for a number of reasons, including personal identification in passports and identity cards, to control the access and presence of public servants, workers and students, and to control attendance at continuous training courses, etc.

2.1 Biometric data processing and the right to physical integrity, bodily privacy and personal data protection.

The Spanish Data Protection Agency has defined biometric data as "*physical aspects which, when analysed, enable the identification of unique characteristics of the individual and which, considering that it is impossible that two individuals will ever have the same characteristics, enable the identification of the individual in question, once processed. Digital fingerprints, the iris of the eye and voice, etc., are used for such purposes*". In this respect, the Working Document of the Article 29 Working Party on Biometrics adopted on August 1st, 2003 is worth a special mention, particularly with regard to definitions. The purpose of the document is to contribute to the effective and homogenous application of the national provisions on data protection adopted in compliance with Directive 95/46/EC on biometric systems[32]. The paper focuses primarily on biometric applications for authentication and verification purposes. As the Working Document of the Article 29 Group indicates "the collection of biometric samples, the so-called biometric data (e.g. image of the fingerprint, picture of the iris or of the retina, recording of the voice), is carried out during a phase called "enrolment" by using a sensor specific to each type of biometrics. The biometric system extracts from the biometric data user-specific features to build a biometric "template". The template is a structured reduction of a biometric image: the recorded biometric measurement of an individual. It is the template, presented in a digitalized form, which will be stored and not the

analysed in TRONCOSO REIGADA, "*Ficheros de perfiles de ADN y derecho fundamental a la protección de datos personales*", in *Estudios sobre Administraciones Públicas y Protección de Datos Personales,* Civitas, Madrid, 2006, p. 36-38.

[32] See art. 4.11) of the Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012 (General Data Protection Regulation), which also defines biometric data: "any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data".

biometric element itself". This Document by the Article 29 Group on biometric data defines biometric systems as "applications of biometric technologies, which allow the automatic identification, and/or authentication/verification of a person".

It should be pointed out that the processing of biometric data is a concern from an ethical perspective[33]. A wide and uncontrolled utilisation of biometrics on the part of the public authorities for purposes other than law enforcement may cause social rejection[34]. The question has been raised as to whether the collection of data of the human body is compatible with human dignity, as this can be interpreted as treating people as if they were machines, reducing them to mere algorithms. From this perspective, the conversion of a binary code of a three-dimensional image of a part of the body, such as the hand, could be considered an offence against human dignity. Nevertheless, as the Ruling of the Contentious-Administrative Chamber of the Supreme Court of 2 July 2007 (speaker Lucas Murillo) rightly points out in relation to the processing of workers' biometric data to control attendance[35], "*the system does not go that far. Reducing a person to a mere number and treating him as such could be considered a violation of that dignity, but this is not the case here. In reality, the acquisition of images and records of different parts of the human body for identification purposes is nothing new. Therefore, photographing the face or the entire body is not considered harmful. The collection of finger or footprints, the recording of the iris and the voice are allowed, and even the collection of DNA in some cases. Furthermore, the use of identification codes is on the increase. Pursuant to Article 3 a) of the Spanish Organic Law, such codes are considered personal data and include personal identification numbers, e-mail addresses and the IP address for data transmission in Internet. These, and the aforementioned parts of the body, are increasingly being collected, filed and used for legitimate purposes and in accordance with the law. It can therefore be concluded that the acquisition of numerical data and personal characteristics is not a violation of the fundamental*

[33] The International Conference of Data Protection and Privacy Commissioners held in Montreux on 16 September 2005 passed a resolution on the use of biometrics in passports, identity cards and travel documents in which it pointed out that the widespread use of biometrics will have a far-reaching impact on the global society and should therefore be subject to an open worldwide debate.

[34] In the document on biometrics, the Article 29 Working Group questioned whether Europeans would allow their fingerprints to be used for other purposes. Furthermore, the issue of people who have more difficulty passing biometric tests and who might consequently be unfairly treated and stigmatised, such as the handicapped, was also raised.

[35] Appeal no. 5017/2003 to the Supreme Court, on fundamental rights, instituted by the Confederación General del Trabajo de Cantabria and the Sindicato de Trabajadores de la Enseñanza de Cantabria trade unions against the Ruling of the Contentious-Administrative Chamber of the Supreme Court of Cantabria of 21 February 2003 giving rise to appeal no. 763/2002, on the installation of a new system for the control of staff working hours using biometric data.

right in question, nor, indeed, is the conversion of a picture of the hand into an automated algorithm a manifestation of the devaluation of the individual in the manner alleged by the appellants".

Nevertheless, the processing of biometric data has to be evaluated from the perspective of fundamental rights. Accordingly, it has been suggested that the conversion of the physical characteristics of a person into a digital identification code and its storage in a database is a violation of the right to physical and moral integrity and physical and medical privacy. However, the use of a part of the body as a means of identification does not cause physical or bodily harm. As Spanish Constitutional Court Ruling 207/1996, of 16 December, points out, slight or serious body intervention would have to take place without the consent of the data subject for this to be considered interference with the fundamental right to physical integrity. The aforementioned right is interfered with when the intervention involves the use of a person's body for research, body searches, the extraction of certain external or internal elements of the human body, the collection of hair, nail or blood samples. This, however, is not the case, or not, at least, to the same extent as the collection of biometric data, such as the fingerprint[36]. Neither is it interference with the right to moral integrity, as the collection and processing of biometric data does not cause humiliation or abasement[37]. Nor is the biometric reading of the hand or iris considered interference with the right to bodily privacy. The Spanish Constitutional Court, in Ruling 37/89 of 15 February, has stated that while bodily privacy is included in the right to personal privacy, this constitutionally protected right does not coincide, it is not co-extensive with the physical reality of the human body. In the Court's opinion, the right to privacy is only interfered with by interventions that violate the dignity or modesty of the individual -in accordance with the criteria established by community culture- because of the parts of the body affected or the instruments used. Consequently, the processing of biometric data of parts of the body that do not affect an individual's modesty is not considered a violation of the right to bodily privacy. Spanish Constitutional Court Ruling 207/1996 supports this assertion when it states that body searches only interfere with the right to privacy if they are conducted on the private parts of the body and affect an individual's privacy -for example, gynaecological check-ups or anal or vaginal searches-. The collection of biometric data does not

[36] Exposing the body to radiation, X-rays, TAC and magnetic resonance has also been considered interference with the right to physical integrity.

[37] On this matter, see the rulings of the European Court of Human Rights of 25 April 1978, the "*Tryer Case*"; of 25 February 1984, the "*Cambell and Cosans Case*"; and of 7 July 1989, the "*Soering Case*".

appear to be a violation of this type of bodily privacy. Finally, no scientific studies have demonstrated that the acquisition of a three-dimensional image of a part of the body, like the hand, by an infrared laser damages the individual's health. Accordingly, daily contact with the scanner used to read biometric data emits no more radiation than the remote control of a television set.

The main legal issues raised by the processing of biometric data for different purposes concerns the fundamental right to personal data protection. Biometric data is of a personal nature. Article 2 (a) of Directive 95/46/EC and Article 3.a) of the LOPD define "personal data" as "any information relating to an identified or identifiable natural person". It appears that biometric data can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person. The biometric system extracts from the biometric data user-specific features to build a unique biometric template. Although the automated algorithm on its own cannot be used to identify an individual, it is capable of identifying natural persons when it is added to a file containing personal information, such as names, surnames and national identification numbers[38]. Indeed the objective of the processing of biometric data is identification. In order to ascertain whether this type of data processing is a violation of the fundamental right to personal data protection, it is necessary to assess compliance with data protection principles and rights and, in particular, evaluate the limitations using the purpose and proportionality principles[39]. Indeed one of the ways to encourage legitimate biometric data processing is to strengthen personal data protection safeguards.

An interesting question is whether the processing of biometric data can be considered special categories of data pursuant to Article 8 of the Directive art. 9 of the Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data- and article 7 of the LOPD, as it involves the processing of data relating to health and racial origin. It is true that biometric systems, like those

[38] Accordingly, when biometric data, such as a template, is stored in such a way that the data controller and other people have no reasonable means of identifying the data subject, the information is not considered personal data. The data subject can only be identified when additional data is available.

[39] The Directive does not apply to personal data considered in isolation, but to the processing of personal data, excluding data processed in the course of a purely personal or household activity. Biometric applications in domestic use are therefore excluded from the scope of the Directive. See also art. 2.2.d) of the Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

used to recognise a facial feature or photograph a person can provide information on health and racial origin in occasional cases. The Article 29 Working Group considers that biometric data processing has evolved from the use of purely physical and physiological-based techniques, which measure the physiological characteristics of a person and do not change over time, such as iris recognition, fingerprint verification, outline of hand patterns, retina analysis, face recognition and ear shape recognition, to behavioural-based techniques, which may change over time, and include body odour detection, gait analysis, voice recognition, hand-written signature verification and keystroke analysis[40]. Furthermore, particular attention should be paid when collecting the raw data from which the biometric templates are obtained[41]. In any case, the main biometric data, such as the fingerprint, merely identifies the individual without revealing additional information. It can therefore be concluded that biometric data cannot generally be considered specially protected data.

The processing of biometric data must comply with personal data protection legislation and, hence, the Community Directive –in the future, the Proposal for General Data Protection Regulation and, in the case of Spain, the LOPD. The drawing up of the codes of conduct provided for in Article 27 of Directive 95/46/EC –art 38 of the Proposal for a General Data Protection Regulation- may also contribute to the application of data protection principles to biometric data processing. There must be a controller of the file to decide on the purpose, content and use of biometric data processing, who is also responsible for declaring the file[42]. In relation to countries exempt from the notification

[40] On this point, the Article 29 Working Group has stressed the need to pay attention to the correlations between certain papillary patterns and corresponding diseases. As, for instance, certain papillary patterns are said to depend on the nutrition of the mother (and thus of the foetus) during the 3rd month of the pregnancy. Leukaemia and breast cancer seem to be statistically correlated with certain papillary patterns. Nevertheless, despite an ongoing scientific discussion on the matter, any direct or precise correlations in these cases are not known.

[41] As is the case when obtaining DNA profiles, which are used only for identification purposes, special attention should be paid at the time of collection, as biological samples contain predictive information, the so-called DNA coding regions. In the case of biometric data also, the enrolment phase plays a key role as it is the only one in which raw data, extraction and protection algorithms (cryptography, hashing, etc.) and templates are all simultaneously present. In the Working Document on biometric data, the Article 29 Working Group states that it is necessary to analyse the extent to which the raw data reveals information that may be regarded as sensitive in the meaning of Article 8 of Directive 95/46/EC. In any event, it should be taken into consideration that raw data cannot be reconstructed using templates.

[42] This notification obligation disappeared in the Proposal for a General Data Protection Regulation 2012. The controller of a fingerprint file for passport and identity card purposes would be the police; the controller of a fingerprint file to control the attendance of public servants would be the corresponding Administration, and that of a private company would be the company itself. In the case of private training centres, which collect biometric data to prove to the Administration that training courses have actually been held and attended, it is understood that the centres themselves are the file controllers, as they process the data on behalf of the data controller, which would be the Administration.

requirement, the Article 29 Working Group has stressed the need to consider the use of biometric systems as a data processing method that carries specific risks for the rights and freedoms of individuals. Such risks, pursuant to Article 20 of Directive 95/46/EC, include the use of the data for purposes other than which it was originally intended and unauthorised access thereto. Accordingly Article 20 of Directive 95/46/EC, such processing shall be subject to the control of the data processing authorities in accordance with national legislation and the national authorities shall be notified prior to introducing biometric data processing systems. The Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012 introduces an obligation of the data controller to do a *Privacy Impact Assessment* (PIA) when data processing involve specific risks to the rights and freedoms of data subjects in view of its nature, scope or purpose. This is the case of biometrics data processing –art. 33.1.d) of the Proposal for a General Data Protection Regulation-.

The principle of prior informed consent, that is to say, the obligation to inform the data subject, must also be complied with. Data processing is only considered legitimate when the data subject is informed of the processing and, in particular, of the collection of biometric data. Articles 10 and 11 of Directive 95/46/EC stipulate that the controller shall inform the data subject of the identity of the controller and the purposes of the processing for which the data are intended[43]. The principle of prior informed consent is important, considering that biometric systems are used to collect data, such as distance facial recognition, fingerprint collection, voice recording and DNA samples, without the consent of the data subject, and enable the identification of the individual when entered on a biometric database[44]. These biometric technologies lend themselves to blanket utilisation on account of their "low-level intrusiveness". Therefore, it seems necessary to lay down specific

---

Such training centres, which we will look at later on, collect biometric data in compliance with the obligation to control attendance at courses.

[43] Article 5 of the LOPD is much more specific. It establishes the obligation to inform the data subject of any possible data transfers; of his right to access, correct and cancel the data; to specify whether data collection is compulsory or optional, and the consequences should the data subject refuse to allow the processing of his data, that is to say, the disciplinary measures that will apply to the public servant who refuses to consent to the processing of fingerprint data.

[44] As the Article 29 Working Group points out, "in applying a biometric algorithm to the fingerprint found on a glass, one may be able to find out if the person is on file in a database containing biometric data, and if so, who he is, by proceeding with a comparison of the two templates. This also applies to other biometric systems, such as those based on keystroke analysis or distance facial recognition, on account of the specific features of the technology involved". See the Article 29 Working Group's Working document on Biometrics.

safeguards in respect of them. The restriction of the principle of prior informed consent is only justified when thus provided for by law and when it constitutes a necessary measure to safeguard the legitimate interests set out in Article 13 of Directive 95/46/EC –article 21 of the Proposal for a General Data Protection Regulation-, that is to say, national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences, or an important economic or financial interest of a Member State or the EU, etc.

It should also be pointed out that biometric data processing must ensure the right to access, correct and cancel the data. Above all, this type of data processing must comply with information security and the obligation to confidentiality. Directive 95/46/EC merely specifies, in Article 17, that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Moreover, he shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. As pointed out earlier, the Directive does not specify the concrete security measures to be adopted; in Spain, basic level security measures must be adopted, pursuant to the Security Regulation passed by Royal Decree 1720/2007 for the processing of non-sensitive data. The necessary security measures should be implemented from the beginning of the processing, and especially during the phase of "enrolment", where the biometric data are transformed into templates or images, to the end, particularly when the information is transmitted via Internet[45]. The Article 29 Working Group states

[45] Article 29 Working Group's Working document on Biometrics points out that the security measures could include, for instance, the encryption of the templates and the protection of encryption keys in addition to access control and protection making it virtually impossible to reconstruct the original data from the templates. Some new technologies should be taken into account in this context. An interesting development is the possibility to use biometric data as encryption keys. This would a priori create less risk for the data subject as it may only be decoded on the basis of a new collection of the biometric data from the data subject himself and so it avoids the creation of databases containing templates of biometric data that have the potential to be reused for unrelated purposes. It has also stressed the importance of security with regard to passports containing biometric data. The Resolution of the European Parliament of 2 December 2004 lays down that the biometric elements of passports shall be stored on "a secure storage medium […]. The storage medium shall have sufficient capacity to guarantee the integrity, authenticity and confidentiality of the data". This position is also supported by the Article 29 Working Party, which points out that the issuer is responsible for the security standards of passports and travel documents and the required infrastructure. Citizens shall not be held responsible for any shortcomings that occur when preparing or issuing the document or during its period of validity. In this respect, the Commission decision of 28 February 2005 is worth a special mention, as it considers that the processing of biometric data for passport purposes creates a lot of risks for the right of privacy of the European citizens. It is not appropriate to safeguard the rights of the citizens, since the contact between the RFID-chip and the reader can be

that it should be understood that any loss of the integrity, confidentiality and availability features in respect of the databases would be clearly prejudicial to all future applications based on the information contained in such databases, as well as causing irretrievable damage to data subjects. For instance, an identity theft, in addition to providing unauthorised access to the services available to the real owner, would make the individual's fingerings unreliable for future applications, thereby limiting his/her freedom[46]. Nevertheless, it appears that the use of biometrics generally improves the protection of personal information because it strengthens the identification and authentication controls that prevent unlawful use of personal data. Accordingly, the inclusion of facial images in biometric passports makes it more difficult to forge them and ensures that the person presenting the passport is in reality the person to whom it was issued.

Another aspect that should be analysed is the principle of prior informed consent and the criteria for making data processing legitimate (Article 7 of the Directive, Articles 6 of the Proposal for a General Data Protection Regulation 2012 and Article 6 of the LOPD). Biometric data processing must be justified in accordance with one of the criteria set out in Article 7 of Directive 95/46/EC – art. 6 of the Proposal for a General Data Protection Regulation-. If the data controller justifies the legitimacy of biometric data processing on the basis of the data subject's consent, this consent must meet the requirements stipulated in Article 3 of the LOPD and Article 2 of Directive 95/46/EC – Article 7 of the Proposal for a General Data Protection Regulation-; that is to say, the data subject's freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. Article 4.8 of the Proposal for a General Data Protection Regulation sets 'the data subject's consent' means any freely given specific,

---

eavesdropped and the information can be skimmed. The risks stemming from of the implementation of RFID-chips in the passports, in other travel documents or in ID-cards, as well as the risks arising from the implementation of biometric features in the chip, need a security architecture which is aimed at providing an increased level of confidence for information to be exchanged. Fully aware of the inherent problems, the Working Party thus sees a need for a global Public Key Infrastructure (PKI). The circumstances under which fingerprints are collected will have to guarantee perfect reliability and the Group has thus recommended the use of a special security mechanism known as the Extended Access Control mechanism. See the Article 29 Working Group's document on Passports.

[46] Taking into consideration the rapid technical evolution and the increased concern for security, many biometrics systems work by combining different biometric modalities of the user with other identification or authentication technologies. Some systems for instance, cumulate face recognition and voice registration. To perform authentication, three different methods may be used jointly – based on something an individual knows (password, PIN, etc.), something an individual owns (token, CAD key, smart card, etc.) and something an individual is (a biometric feature). For instance, with a computer, one could insert a smart card, type a password and present his/her fingerprint. See the Article 29 Working Group's document on Biometrics.

informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being Processed".

The most common procedure will be the processing of biometric data without the data subject's consent on the basis of other criteria for the legitimacy of data processing. When biometric data is collected by a Public Administration, the data subject's consent is not required when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 7 (e) of Directive 95/46/EC; Article 6.1.e) of the Proposal for a General Data Protection Regulation 2012). Consequently, Article 6.2 of the LOPD stipulates that personal data may be collected without the data subject's consent "for the performance of the functions of the Public Administrations within the scope of their powers or competencies"[47]. This would be the case, for example, when biometric data is collected for the purpose of issuing a national identity card or passport, when civil servants' data is collected to monitor attendance at work, or to monitor the attendance of participants on publicly-funded training courses. On this point, it should be mentioned that the Ruling of the Contentious-Administrative Chamber of the Supreme Court of 2 July 2007 (speaker Lucas Murillo) justifies the processing of fingerprints to monitor the working hours of civil servants on the basis that observance of working hours is an inherent obligation to the relationship binding civil servants to the Administration and that Article 6.2 of the LOPD exempts the latter from the obligation to seek their prior consent in such cases[48]. Likewise, in the Supreme Court's opinion,

[47] Article 6.1 of the LOPD stipulates that "the processing of personal data shall require the unambiguous consent of the data subject, unless otherwise stipulated by law". Article 6.2 sets out that "consent shall not be required when personal data is processed for the performance of the functions of the Public Administrations within the scope of their powers; when processing is necessary for the performance of a business, employment or administrative contract or memorandum of understanding to which the data subject is party; when necessary to protect the vital interests of the data subject under the terms set out in Article 7, section 6 of this Law; when the data is accessible to the public and processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, provided the fundamental rights and freedoms of the data subject are not violated".

[48] Nevertheless, the Spanish Data Protection Agency understands that no exemptions are allowed from the obligation to obtain the data subject's consent when data "is collected for the performance of the functions of the Public Administrations within the scope of their powers" and that a law must exist therefor, considering that, pursuant to Constitutional Court Ruling 292/2000, the processing of personal data on the part of the public administrations without the data subject's consent is subject to the principle of legal reserve set out in Article 53.1 of the Constitution. Accordingly, the public administrations shall not process biometric data unrestrictedly. Such processing must be provided for by a regulation with the status of a law in the broad sense envisaged by the Spanish Data Protection Agency, or must at least be necessary to ensure compliance with a legal obligation, pursuant to the terms set out in Article 6.2 of Organic Law 15/1999. In the Spanish Data Protection Agency's opinion, exemption from the obligation to obtain the data subject's consent to process biometric data in order to monitor attendance at work is allowed because

there is no regulation that prohibits the use of the chosen technology to monitor the observance of working hours. It is not harmful to the aforementioned fundamental rights by virtue of its novelty or complexity.

Another important circumstance where the obligation to obtain the data subject's consent prior to data processing is not required is when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 7 (b) of the Directive); Article 6.1.b) of the Proposal for a General Data Protection Regulation). Spanish legislation has interpreted that processing involves the parties to a business, employment or administrative contract or memorandum of understanding. This applies to the collection of biometric data on the employees of private entities. In other cases, personal data processing is justified in the exercise of administrative functions, as well as the existence of a business relationship. This is the case, for example, when biometric data processing is used to monitor the attendance of students at training courses, in which case it is necessary for the performance of an administrative control and supervisory function and because there is a relationship between the Administration that organises the training course and the person who undertakes to attend it, and not because there is a relationship between the Administration and the private centre that receives the subsidy to give the training.

In accordance with the Directive, data processing without the data subject's consent is also justified when it is necessary for compliance with a legal obligation to which the controller is subject (Article 7 (c), Article 6.1.c) of the Proposal for a General Data Protection Regulation). The LOPD also stipulates that data processing is allowed in this instance when so stipulated by law. There are many circumstances in which the law provides for the exemption from obtaining the data subject's consent. This is particularly the case with Law 59/2003, of 19 December, on the electronic signature, which envisages the Electronic national identity card[49]. When biometric data is processed in compliance with a legal provision, the Constitutional Court shall decide whether it is compatible with the principle of proportionality. On the other hand, if processing is carried out in compliance

---

there is a legal relationship between the data controller and the data subject, which entitles the former to control the latter's compliance with legal obligations.

[49] We have referred to this matter in the Presentation on *e-Prodat: e-Government and data protection in European Regions and Cities*, Madrid, 2006.

with the exercise of an administrative function or legal relationship, the Data Protection Agencies may analyse the proportionality of the interference with the fundamental right to personal data protection. On occasions, the legislation does not expressly provide for the processing of biometric data but sets out a number of legal obligations that may take different forms. Consequently, the legislation on subsidies, which governs the control of public funds, may be interpreted as a legal entitlement to process personal data for the purpose of monitoring attendance at subsidised courses. Likewise, the Civil Service Basic Statute stipulates the legal obligation to observe the working hours and may allow the monitoring of attendance through the processing of personal data. Nevertheless, this legislation does not expressly provide that attendance be monitored through the use of biometric data processing.

2.2 Biometric data processing and the principles of data quality and proportionality.

The legitimacy of biometric data processing is mainly assessed using the principle of data quality and, in particular, the principle of proportionality. The principles relating to data quality are set out in Article 6 of Directive 95/46/EC -Article 5 of the Proposal for a General Data Protection Regulation- and in Article 4 of the LOPD. This article stipulates "*personal data shall only be collected for processing purposes and processed when it is adequate, relevant and not excessive in relation to the explicit and legitimate purposes for which it is collected and/or further processed*" (Article 4.1). It is therefore important that the biometric data collected is restricted to the minimum required to identify the data subject, and excessive data should not be collected or processed[50]. It is important that the database where the biometric data is stored does not contain additional information on the user. Moreover, it shall not be possible to identify the individual using the encoded binary data on its own. It should be mentioned that the use of biometric systems might be

[50] To prevent excessive data processing, the Article 29 Working Party is of the opinion that for access control purposes (authentication/verification), biometric systems related to physical characteristics which do not leave traces (e.g. shape of the hand but not fingerprints) create less risks for the protection of fundamental rights and freedoms of individuals.

constructed in such a way that they could be considered as privacy enhancing technology inter alia because they may reduce the processing of other personal data like name, address, residence, etc.[51]

Compliance with the principle of data quality and the prohibition to process excessive data ensures that biometric data is not stored on central databases unless necessary. It should therefore be determined whether storage is necessary and on what medium prior to conducting biometric data processing. The storage of biometric data on an object exclusively available to the user, such as a microchip card, is less intrusive and poses fewer risks for the protection of fundamental rights of individuals than data that is memorised in third-party control access devices or in central databases[52]. Applications that do not involve the storage of biometric data on central databases should therefore be used for authentication and verification purposes[53]. Conversely, identification can only be achieved by storing the reference data in a centralised database, because the system, in order to ascertain the identity of the data subject, must compare his/her templates or raw data (image) with the templates or raw data of all persons whose data are already centrally stored[54]. In any event, the amount of raw data (the original image) and biometric data collected should be restricted to the minimum required or the intended purpose.

---

[51] The Article 29 Working Party document highlights the importance of privacy-enhancing technologies that keep the among of data collected and the risk of unlawful processing to a minimum.

[52] The Article 29 Working Party document states that an additional issue that is also important from a data protection point of view is the form of the storage of users' templates. The templates can be stored in the memory of a biometric device, in a central database or in plastic cards, optical cards or smart cards. The Working Party stresses the importance of using devices that do not involve storage in central databases or memorise the traces on control access devices. See the Article 29 Working Party Document on Biometrics.

[53] As the Article 29 document points out, the difference between authentication (verification) and identification is important. Authentication answers to the question: Am I the one I pretend to be? The system certifies the identity of the person by processing biometric data which refer to the person who asks and takes a yes/no decision (1:1 comparison). Identification answers to the question: Who am I? The system recognises the individual who asks by distinguishing him from other persons, whose biometric data is also stored. In that case the system takes a 1-of-n decision, and answers that the person who asks is X.

[54] On this point, we should mention the legislative decision of the European Parliament of 2 December 2004 which required the prohibition of a central database of European Union passports and travel documents containing the biometric and other data of all EU passport holders. The Working Party supports this demand and states that the objection against a European central database of European Union passports and travel documents are the same objections against national central databases of passports and travel documents as well as against central databases for ID-cards. There is a risk that the setting up of a centralised database containing personal data and in particular biometric data of all (European) citizens could infringe against the basic principle of proportionality. Article 29 Data Protection Working Party, Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Official Journal L 385, 29/12/2004 p. 1 - 6). Adopted on 30 September 2005.

Directive 95/46/EC prohibits further processing that would be incompatible with the purpose for which the data was collected. The LOPD stipulates that "*personal data shall not be processed or used for purposes that are incompatible with the purposes for which the data was collected*" (Article 4.2). It should be pointed out that biometric data, such as fingerprints, that is collected for a specific purpose, such as identification and to control access or attendance, shall only be used for this particular purpose and not, for instance, for surveillance in the workplace[55]. Therefore, all measures must be taken to prevent such incompatible re-use[56]. On this point, it should be stressed that centralised storage of biometric data increases the risk of unlawful use, as well as the use of biometric data as a key to interconnecting different databases[57], facilitating the interoperability of different systems and the configuration of profiles of an individual's habits[58]. Article 4.7 of the LOPD sets out the prohibition to "collect data through fraudulent, unfair and unlawful means". The collection of biometric data without informing the data subject that the data will be processed, specifying the purpose, the name and address of the data controllers and of his/her rights may constitute fraudulent, unfair and unlawful processing. As pointed out earlier, one risk of biometric data processing is that the data can be obtained through the physical traces left by people without their knowledge, and data may therefore be collected without the data subject's consent. For data processing to be considered fair and lawful, the raw data must be obtained directly from the data subject and with his/her consent.

---

[55] The CNIL believes that the shape of the hand is data that does not lend itself to re-use for purposes other than those for which it was originally collected. The shape of the hand does not leave traces, like the fingerprint, thus preventing the data from being used for other purposes.

[56] Directive 95/46/EC and the Proposal for a General Data Protection Regulation provide for exemptions to the prohibition to further process data for incompatible purposes but specific conditions apply.

[57] The processing of digital fingerprints would also enable the identification of individuals in different circumstances and is therefore potentially capable of being used for unintended purposes. The CNIL confirmed this assertion, stating that a digital fingerprint file makes persons traceable and may be used for purposes other than originally intended. The Greek Data Protection Authority is of a similar opinion, stating that "due to the proportionality standard (which involves a balance of interests), the processing of digital fingerprints is allowed only in exceptional circumstances (fingerprints could be misused for other purposes than originally intended and make individuals traceable)".

[58] The Resolution of the European Parliament of 2 December 2004 points out that "the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets." The Article 29 Working Party document also points out that "if society encourages the development of fingerprint or other biometric databases for further routine applications, it may increase the potential re-use by third parties as an element of comparison and research in the framework of their own purposes, without such an objective having initially been sought; these third parties may include law enforcement authorities. It is generally accepted that the risk of the reuse of biometric data obtained from physical traces unknowingly left by individuals (i.e. fingerprints), for incompatible purposes is relatively low if the data is not stored in centralised databases, but remains with the person and is inaccessible to a third party".

The principle of data quality requires that the data is accurate and up-to-date. Biometric data does not need to be updated because it does not change over time. Nevertheless, the accuracy of biometric data is extremely important. There is a common belief that biometric systems are an infallible means of identifying and authenticating individuals, which is not always the case. Biometric system errors have serious consequences for the individual in, for example, the case of passports, as they may mistakenly allow un-authorised persons to enter a country and refuse entry to an authorised individual, and it is difficult to prove otherwise. A prospective study commissioned by the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament has stressed that there should be additional procedures in place for the identification and authentication of individuals apart from biometrics, as biometric systems are not always correct or accessible to everyone. These additional procedures would respect the rights of individuals who are unable to complete the registration process, and who should not be penalised for the shortcomings of the system[59].

The principle of data quality requires that only the persons authorised by virtue of their functions and powers have access to personal information. Biometric systems shall consequently ensure that only authorised persons have access to biometric data. This is particularly important in the case of passports and identity cards, and it is therefore required that registers, containing a record of the authorities and bodies authorised to access biometric databases, are in place[60].

The principle of data quality also requires that personal data be "*deleted when no longer necessary or relevant for the purpose for which it was collected or registered*". Personal data must therefore be deleted once the purpose for which it was collected has been fulfilled, and the data may be blocked until the prescribed period has elapsed. Therefore, biometric fingerprint data used to monitor attendance has to be erased not only when the employment relationship has ended, but also when attendance has been verified. All unnecessary biometric records shall be deleted as soon as

---

[59] When refused entry at a border control or other controls conducted by the competent authorities, the individual concerned shall be informed of the reasons for refusing entry, the channels through which he/she may express his/her opinion and the authorities to whom he/she may appeal.

[60] For this reason the Article 29 Working Party has supported the European Parliament's request that each Member State keep a record of the competent authorities and authorised bodies, in accordance with Article 3 of Regulation (EC) No 2252/2004. The Member States shall notify the Commission of this registry and, when necessary, of the regular updates thereto. The Commission shall keep an up-to-date record and publish a list of the national registers once a year.

possible[61]. If the data is to be stored for statistical purposes, the information must first be depersonalised.

We will now assess compliance with the principle of proportionality, which is an element of the principle of data quality itself[62]. The processing of biometric data constitutes a restriction of the fundamental right to personal data protection and, like any interference with a fundamental right, must be assessed using the principle of proportionality[63]. Compliance with this principle requires taking the type of data and the intended purpose of processing into account, such as identification in passports and other documents, to monitor the attendance at work of employees of public and private entities, attendance at publicly-funded training courses, educational institutes, etc. There is no single solution with regard to the proportionality of biometric data processing. However, the objective pursued and the constitutional value it aims to achieve must be taken into consideration in each specific case in order to distinguish the reasonable use of biometric data from unlawful use and to be able to reduce the social risks involved. The solution that is most in keeping with constitutional requirements is the processing of data on the grounds of important public interest, while interfering as little as possible with the fundamental rights of individuals. It should be stressed that nothing can replace compliance with the principle of proportionality in personal data processing. The existence of other legitimate reasons, including the data subject's consent, do not grant exemption from the principle of proportionality. The data subject's consent does not make unlawful processing, that is to say, processing that does not comply with the principle of proportionality, lawful[64]. Indeed proportionality has been the main criteria used in almost all resolutions adopted to date by the data protection authorities charged with determining the legitimacy of biometric data processing[65].

---

[61] Consequently, in the case of biometric data processing in Banc de France, the CNIL established that the data could only be stored while the person was employed by Banc de France and that personal information would be deleted after three months.

[62] The principle of proportionality is, in short, a requirement of the principle of data quality, that is to say, that biometric data may only be used when it is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.

[63] See Constitutional Court Rulings 37/1989 and 207/1996. We cannot agree in this case with the statement contained in the Supreme Court Ruling, of 2 July 2007 (F. J. 8º), when it says that "it is difficult to disagree with the Treasury Ministry when it says that when fundamental rights are not restricted, failure to observe the constitutional doctrine on proportionality cannot be upheld".

[64] Furthermore, as we will see later on, there is no free consent in the workplace, as the employment relationship is an intrinsically unequal one.

[65] This is the case with the French, German, Italian, Greek and Portuguese authorities.

In relation to the principle of appropriateness, it should be pointed out that biometric data processing complies with the principle of appropriateness because this restriction of fundamental rights is appropriate for achieving the aforementioned objectives. Problems mainly arise when assessing whether the processing of biometric data complies with the principles of necessity and proportionality in the strict sense. The legitimate purposes cannot be achieved at any cost. It is therefore important to determine the legitimacy of biometric data processing by evaluating whether the objective pursued can be achieved by a less intrusive means, that is to say, whether equally effective measures, which are less harmful to the individual, can be used to achieve the same objective. It is also necessary that the measure, once it has been decided that it is necessary, is proportionate to the proposed objective, and this requires reaching an acceptable compromise between the objective pursued and interference with the fundamental right to personal data protection.

The processing of biometric data for identification purposes complies with the principle of proportionality[66]. It complies with the sub-principle of necessity because other, less harmful measures are incapable of facilitating the identification of individuals with the same level of effectiveness. Advances in identification technology have made more reliable identification methods available, such as biometric data processing of the facial image and the digital fingerprint. It also complies with the sub-principle of proportionality in the strict sense, as the measure adopted, that is to say, interference with the fundamental right to personal data protection, is proportional to the proposed objective, i.e., the identification of citizens[67]. Consequently, the Council of Europe adopted Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security

---

[66] On 11 September 2001, biometric technology was deemed an appropriate means of improving public security. Consequently, the European Union initiated a debate on the use of biometrics in identity cards, passports, travel documents and visas. LO Convention No. 108 was amended in 2003 in order to introduce compulsory biometric identity documents for seafarers. This has also been discussed at other international forums, such as G8 and the OECD.

[67] However, as pointed out in the Analysis and impact study on the implementation of Directive EC 95/46 in Member Status, loc. cit., commissioned by the European Commission, in Greece, the data protection authority issued a decision relating to biometric data in identity cards for Greek citizens. The decision was, amongst others, based on the Law 2472 and the Directive 95/46/EC. In its decision the Data Protection Authority held that '[a]ny processing of personal data which exceeds the pursued purpose or which is neither appropriate nor necessary for the achievement of such purpose is considered to be unlawful. The purpose of identity cards is to verify the identification of the data subject. On these premises, the Data Protection Authority held that the processing of a number of personal data on identity cards would exceed the said purpose: Most relevant for the scope of this study are fingerprints. They were held not to be necessary for the purpose of verifying identity (which is evident from the photo) and, in addition, were held to offend human dignity. The decision further stated that the processing remains unlawful even in situations where the data subject has given his consent.

features and biometrics in passports and travel documents issued by Member States. Article 1.2 of the said Regulation stipulates that passports and travel documents shall contain a facial image and fingerprints[68]. Up until then it was sufficient to include a description of a few biometric features in passports and other travel documents, such as a photo, the gender, height or colour of the eyes. Pursuant to Regulation (EC) No 2252/2004, European citizens are obliged to provide digital biometric data, which is subsequently stored in databases[69]. The objective of the aforementioned Regulation was to render passports more secure by means of a legally binding instrument on standards for harmonised security features and at the same time to establish a reliable link between the genuine holder and the document by introducing biometric identifiers. In addition, this would allow EU Member States to meet the requirements of the US Visa waiver programme in conformity with international standards. The Council adopted Regulation (EC) No 2252/2004 on the basis of the draft of the Justice and Home Affairs (JHA) Council of 25-26 October 2004[70], diverging from the Commission's initially more moderate stance[71] and the openly restrictive policies of both the European Parliament[72] and the Article 29 Working Party[73]. Countries that issue identity cards have

---

[68] Accordingly, the European Union considers that the processing of fingerprints is not contrary to data protection legislation and complies with the principle of proportionality.

[69] The German data protection authority has handed down a favourable decision on the introduction of biometric characteristics on identity papers in order to prevent their falsification, provided that the data are stored in the microchip of the card rather than in a database for comparison with the owner's fingerprints. See the Article 29 Working Party's document on Biometrics.

[70] The European Council of Thessaloniki, on 19 and 20 June 2003, confirmed that a coherent approach is needed in the European Union on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems (VIS and SIS II). As a result of the JHA Council on 25-26 October 2004 the text of the proposal was changed to envisage both biometric features in a mandatory way.

[71] In this draft the European Commission proposed that passports and other travel documents should include a storage medium with a facial image in a mandatory manner. The Member States were allowed to implement fingerprints into the passports by national law. Furthermore, the European Commission proposed that the biometric identifier shall be stored on a storage medium with sufficient capacity. It could be a contactless chip but it may also be another storage medium with the capacity required. The draft Regulation also offers the possibility to store fingerprints in a national database with a view to a future European Register of issued documents.

[72] The European Parliament legislative resolution of 2 December 2004 on the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports supported the introduction of biometric data with the facial image in passports. However, it rejected the mandatory inclusion of the fingerprint and the establishment of a central database of European Union passports and travel documents containing all EU passport holders' biometric and other data, alleging that this was a breach of the principle of proportionality and a violation of the right to privacy and data protection. Furthermore, the legislative resolution of 2 December 2004 stipulates that the biometric features in passports shall be used only for verifying the authenticity of the document and the identity of the holder and that the passport shall include a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored. It also declares that the storage medium may be used only by the competent authorities of the Member States for reading, storing, modifying and erasing data.

[73] Likewise, the Article 29 Working Party strictly opposes the storage of all EU passport holders' biometric and other data in a centralised data base of European passports and travel documents. It points out that the purpose of introducing

considered the inclusion of biometric data therein. Spain introduced the processing of biometric data for the issuance of the Electronic national identity card and passport pursuant to the revision set out in Royal Decree 896/2003, of 11 July, where Article 10.5 stipulates that "*the biometric data required to further facilitate identification of the holder may be included in either the personal data page, referred to in Section 2 of this Article, or any other area determined by the Ministry of the Interior*"[74]. It should nevertheless be mentioned that the implementation of biometric features in passports, other travel documents and ID-cards raises a lot of ethic, legal and technical questions, and that if such a measure is adopted, effective safeguards have to be implemented[75].

The processing of biometric data for the purpose of monitoring the attendance of civil servants is justified on the basis that they have a special relationship of subjection with the Public

---

biometric features in passports and travel documents as defined by the Regulation has to be explicit, appropriate, proportionate and clear. The Member States should guarantee in a technically sound way that the passports include a storage medium with sufficient capacity and the capability to guarantee the integrity, the authenticity and the confidentiality of the data. The Regulation should define who may have access to the storage medium and for which purposes (reading, storing, modifying or erasing data). The Member States shall set up a register of competent authorities. Stefano Rodotá, who was at this time the Chairman of the Working Party, argued against a second mandatory biometric feature. The Chairman stressed that the introduction of an additional biometric feature makes it all the more necessary to create a secure and waterproof system making sure that the fundamental right of privacy is not endangered. He also stressed the need to set up the appropriate safeguards for the processing of biometric data. In addition, the International Conference of Data Protection and Privacy Commissioners held in Montreux on 16 September 2005 adopted a Resolution on the use of biometrics in passports, identity cards and travel documents. It called for a strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations and for contractual purposes on the basis of consent. Furthermore, it called for the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder when presenting the document.

[74] In accordance with Article 6 of Council Regulation (EC) No 2252/2004, this entered into force on 18 January 2005. The aforementioned Article stipulates that Member States shall apply this regulation: "a) as regards the facial image, at the latest 18 months and b) as regards fingerprints, at the latest 36 months following the adoption of the measures referred to in Article 2". Following Council Regulation (EC) 2252/2004, the Commission has adopted on 28 February 2005 the Decision C(2005)409 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, which refers to Article 2 of Council Regulation (EC) No 2252/2004. The Member States undertook to include a digital facial image in citizens' passports prior to 28 August 2006 and fingerprints prior to 28 February 2008.

[75] The Article 29 Working Group believes that before implementing biometric features in passports, other travel documents or ID-cards, there must be an exhaustive discussion in society. For this purpose, the Committee set up by Article 5 of Regulation (EC) 2252/2004, which is to be assisted by experts appointed by the Article 29 Working Party, will have to present a Protection Profile. The Working Group has called for compliance with a number of conditions: a strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations and for contractual purposes on the basis of consent; the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder when presenting the document; the European Commission and the Member States should guarantee that passports of European citizens including data of fingerprints could not be read by readers that could not support Extended Access Control; it should be guaranteed that only competent authorities are able to have access to the data stored in the chip. Member States shall set up a register of competent authorities.

Administration, and that the purpose of the latter, that is to say, to serve the public, requires that civil servants observe the working hours. It is necessary to ascertain whether this interference complies with the principle of necessity, that is to say, whether a more moderate measure can be taken to achieve the same objective with the same level of effectiveness. This requires that other measures that are less harmful to fundamental rights be sought to ensure that civil servants observe the working hours, such as the traditional access control and signature system, for example. It can only be concluded that the processing of biometric data complies with the principle of necessity if such systems have been installed and have failed to monitor attendance and prevent fraud. Finally, an assessment of the principle of proportionality in the strict sense has to be conducted. This entails an evaluation of whether the level of interference with the fundamental right is balanced and results in more benefits and advantages to general interest than harm to the individuals concerned. In our opinion, the processing of biometric data is a balanced measure for ensuring the attendance of civil servants and, thus, the performance of administrative activities that benefit the general interest. Bear in mind that biometric data merely identifies a person, it is not specially protected data, and the purpose, i.e., to ensure the provision of a public service, is a very important constitutional value. This restriction of the fundamental right to personal data protection provides more advantages for the general interest than damage to other constitutional values. Therefore, the processing of biometric data to ensure the attendance of civil servants complies with the principle of proportionality.

Evaluating the processing of biometric data to monitor attendance at training courses in light of the principle of proportionality is more complex. The sub-principle of necessity requires that the measure, that is to say, the restriction of the fundamental right to personal data protection, is necessary to achieve the proposed objective and that no other, less extreme measure can achieve the objective with the same level of effectiveness. It therefore requires that other measures, which do not involve the processing of biometric data, have been taken and have proven ineffective in achieving the objective. The different central and regional governments of Spain have tried different methods to prove that public-funded training courses have been given and attended and all have failed to prevent fraud. Managing the budget and resources allocated to training requires that the attendance of students be monitored in a reliable manner. Indeed this is a requirement of the European Commission, considering that several of these courses are financed with Community funds. Failure to meet such requirements has given rise to negative rulings by the European Union in

the past. Hence, the Public Administration must adequately control public expenditure and prevent fraud using an equally effective method that interferes as little as possible with the fundamental right to personal data protection. It would appear that up until now no other method that is less harmful to the fundamental right in question can achieve this objective. Hence, the processing of biometric data in this case complies with the principle of necessity because no other measure, which is less harmful to the fundamental right, can fulfil the purpose.

It is necessary to evaluate this interference in light of the principle of proportionality in the strict sense. This requires that the processing of biometric data, that is to say, the restriction of the fundamental right to personal data protection, is proportionate to the proposed objective, taking into consideration the nature of the harmed right, the intensity of the interference and the constitutional value it aims to achieve. In our opinion, the processing of basic personal information for identification purposes, such as a biometric fingerprint, is proportionate to the constitutional value of ensuring that public funds are used efficiently, preventing fraud and facilitating administrative activity in the area of subsidies and aid. On this point, it should be noted that the Court of Justice of the European Communities and the Spanish Constitutional Court have stressed the importance of controlling the use of public funds. The ECJ has pointed out that the obligation imposed by national legislation to communicate and publish data relating to professional income is not a violation of Directive 95/46/EC, provided it can demonstrate that the extensive disclosure of the names of the beneficiaries is necessary to ensure the effective management of public funds, and this must be verified by the national legal bodies. Accordingly, in the Stauder Case, the ECJ ruled that requiring the names of the beneficiaries of a community scheme for the distribution of butter at reduced prices without their consent was justified and an appropriate measure to ensure that individuals who did not quality for the scheme did not benefit therefrom. Likewise, the Spanish Constitutional Court upheld that the constitutional duty to pay taxes, pursuant to Article 31 of the Spanish Constitution, is a legitimate purpose and a sufficiently important constitutional duty to require the imposition of a restriction on the fundamental right to personal data protection. This duty requires that everyone contribute to public expenditure in accordance with their economic capacity, and this involves

ascertaining individuals' economic capacity without their consent[76]. Hence, the processing of biometric data to monitor attendance at training courses complies with the principle of proportionality in the strict sense, as it provides more benefits and advantages to general interest than harm to the individuals concerned.

Furthermore, the processing of the fingerprints of students at collaborative centres of the Public Administration in order to monitor attendance is consistent with the legal obligations of the former. Subsidies are granted subject to the beneficiary fulfilling a number of legal obligations, one of which is to "*prove to the granting body or, when applicable, collaborative entity, that the requirements and conditions have been met, that the activity has been conducted and the purpose of the subsidy fulfilled*"[77]. Indeed, if the beneficiary fails to fulfil these obligations, it is obliged to partially or totally return the subsidy. The rules for the granting of subsidies to run training courses include the monitoring of student attendance by means of a system determined by the granting body. Should the number of students decrease during the course, the beneficiary shall receive a smaller subsidy, in accordance with the subsidy rules.

Nevertheless, the quest for effective use of public funds cannot always be used as a pretext for the use of biometric data, particularly fingerprints, and this belief is not compatible with the fundamental right to personal data protection. Exploitation of this theory could lead to the indiscriminate processing of fingerprint data by the Public Administrations on the pretext of ensuring greater efficiency in public expenditure. While the measure seems to be proportionate in the strict sense, biometric data processing has to be essential for the purpose of monitoring attendance, and no other measure that is capable of fulfilling the same purpose but is less intrusive on the right to personal data protection should exist. This therefore requires that the Public Administration put forward special arguments when communicating data processing.

---

[76] See Constitutional Court Ruling 143/1994, of 9 May. Prior to this, the Constitutional Court had pointed out that there was no absolute right to withhold the financial information required for tax purposes (Constitutional Court Ruling 76/1990).

[77] Article 14.1 b) of General Law 38/2003, of 17 November, on Subsidies.

The issue of biometric data processing to monitor the attendance of employees of private entities has also been raised. In this case, exemption from the obligation to obtain the data subject's consent is not justified by the existence of an administrative function, but by the existence of an employment relationship, the maintenance of which requires the processing of personal data. Again, it should be pointed out that this measure complies with the principle of appropriateness, as the restriction of the fundamental right to personal data protection fulfils the legitimate purpose of monitoring employee attendance at work. Again, however, ascertaining whether it complies with the principles of necessity and proportionality in the strict sense is more complex. When assessing whether interference is necessary, demonstrating that employee attendance cannot be monitored by another method that is less harmful to their fundamental rights is essential. Most companies probably use systems other than biometric ones to ensure employee observance of working hours and biometric methods are probably not necessary in most cases. In this instance, the approach is more restrictive than when it concerns the monitoring of civil servants' attendance. Experience has shown that some public administrations do not ensure compliance with working hours using traditional methods because the permanence of public employment and the unlikelihood of accidents in the workplace have led to a more relaxed control of staff, which is not the case in private enterprise, where the monitoring of employee attendance using less intrusive methods is allowed, and this measure, therefore, does not comply with the principle of necessity. Finally, when determining whether the processing of biometric data of employees in private entities complies with the principle of proportionality in the strict sense, the two constitutional rights, the fundamental right to personal data protection on the one hand, and freedom of enterprise and right to monitor compliance with working hours, pursuant to the employment relationship, on the other, have to be assessed to ascertain whether the restriction is proportionate to the objective pursued. In the case of private enterprise, the performance of administrative activities that benefit the general interest and a special relationship of subjection with the Public Administration do not exist. Hence it is more difficult for the processing of biometric data to comply with the principle of proportionality in the strict sense. Nevertheless, the processing of such data to control access to certain areas of the company for security purposes could be considered proportionate.

The European Data Protection Authorities, with the exception of the British Commissioner, have been quite strict with regard to the use of biometric data to control access and attendance, believing that it is not a proportionate measure for the prevention of fraud in the use of bankcards or public

and private employee attendance at work. Consequently, its use is only authorised in sensitive areas where confidential information is stored or in high-security areas[78]. The restrictive stance taken by

---

[78] "*In Italy, concerning the use of biometric devices, the Garante clarified the lawfulness of the use of digital fingerprints by banking institutions. Encrypted fingerprint recognition systems are only allowed if the use of such systems relates to particular risks which are being faced by the bank; personal data, originating from the fingerprint recognition system, is not filed and collected in a database; the access by means of fingerprint recognition system is voluntary, consensual and not the only way to enter a bank; the data is protected by an encryption system; data may only be decrypted by certain public authorities for the purpose of investigating criminal offences and encrypted data is deleted after one week.* See "Rilevazioni biometriche in banca" (28 September 2001).
The Greek authority asserts that processing of personal data shall be based on the principle of proportionality which means that more moderate means, achieving the same purpose, should be used. Generally, fingerprints are taken by law enforcement agencies on the basis of legislative provisions. The Data Protection Authority ruled that taking fingerprints to monitor the presence of workers would not be proportionate and carry less weight than the individual's right to privacy. Only in exceptional circumstances (such as access to confidential files or high-security areas, safety requirements, etc.), might taking of fingerprints at the workplace be acceptable. The Data Protection Authority further stated that taking fingerprints is unlawful insofar as it exceeds the purpose, and, as a consequence, it could not be justified by individual consent of the data subject.
The CNIL issued some decisions on the use of digital fingerprints as a means of controlling access to facilities. The Avis 'Banque de France' (1997) dealt with access control for high security zones by means of digital fingerprints and codes. Another Avis (2000) dealt with the request made by a Préfecture that wanted to use digital fingerprints (in connection with a personal badge) to control working hours of staff. The digital fingerprint would prevent fraudulent use of badges by colleagues. The registration of digital fingerprints would allow identification of persons in various circumstances and was therefore said to be potentially capable of being used for other purposes than for those for which it was initially designed. The CNIL had to decide whether a database of personal data, which allows the identification of persons, was proportionate to the aims sought. According to the CNIL, the creation of a database containing digital fingerprints was not proportionate to the aim of preventing fraudulent use of badges by other members of the staff.
A further Avis (2000) related to a request made by the Ministry of Education that wanted to set up a system of access control to buildings for the educational staff. The intention was to use digital fingerprints. The aim was to guarantee secure access to those buildings (without the need to distribute badges among the personnel) and not to control working hours (time and data of access would not be registered). According to the general statement of the CNIL: 'Le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations dans lesquelles l'authentification ou l'identification des personnes doit être parfaitement assurée.' The CNIL repeated a former statement saying that a database of digital fingerprints makes persons traceable and may be used for other purposes than those for which it was originally intended. Under these circumstances the CNIL required the biometrical technologies to be adapted and proportionate to the aims sought.
Another Avis (2001) was issued upon a request made by the Louvre. The Museum wanted to set up a biometrical access control, which would identify the contours of the hand. The aim was to control working hours of staff and guarantee security of access. It was intended that the data (on individuals) would only be stored as long as the individual would be employed by the Louvre. Access data (date, time) would be stored for one year. The CNIL concluded that the contours of the hand do not constitute data which is likely to be used for other purposes than those for which it was initially set up. Contours of the hand do not leave traces (e.g. like digital fingerprints) which prevents the data from being used for other purposes.
The Avis 'URSSAF' (2002) dealt with the processing of digital fingerprints used as access control to buildings in Corsica. The CNIL stated that digital fingerprints could potentially be used for other purposes than those for which they were initially constituted, and therefore other means of biometric access control were preferable. The system in Corsica would only concern a few people and give access to a single floor in a building which is guarded by other means. The system would not be able to prevent terrorist attacks to which the Radio station has been subject in the past. Since this measure would not prevent access to buildings by unauthorised persons, the CNIL rendered a negative avis.
The Portuguese Data Protection Authority also took an unfavourable stance to a university's plan to use biometric data (digital fingerprints) to monitor the regularity and punctuality of non-teaching staff, stating that the use of such systems was disproportionate to the aim sought. In contrast, the British Data Protection Authority allows the use of digital fingerprints to monitor presence when the necessary safeguards are in place". This information is taken textually from

the data protection authorities and the Article 29 Working Party comes as no surprise. Nevertheless, it could be more balanced and take all of the legal interests into consideration[79]. As pointed out earlier, the Administration and the legislators of the European Union and Member States do not always take a restrictive stance, but tend to take a balanced view, which was the case, for example, with the processing of biometric data for passports, which initially encountered similar opposition.

Finally, we have yet to analyse the processing of biometric data to monitor the presence of students at schools and universities. It is very difficult to reconcile this type of data processing with the principle of proportionality, both from the point of view of the sub-principle of necessity and the principle of proportionality in the strict sense. There are undoubtedly other methods that are less harmful to fundamental rights and which are equally suitable for monitoring attendance at schools. Above all, however, this measure fails to comply with the principle of proportionality in the strict sense. We are not looking at two constitutional rights or duties of a similar value, hence the processing of biometric data in this case does not pass the cost-benefit analysis[80]. It seems clear that the aim sought, that is to say, to monitor non-attendance in schools, does not justify interference with the fundamental right to personal data protection. It is disproportionate, contrary to the principle of data quality, and, therefore, constitutes a violation of the aforementioned fundamental right[81]. There is concern in the area of education that the frequent use of biometric data may make citizens less aware of the risks associated with the use of such systems[82].

AnFor more information, see the *Analysis and impact study on the implementation of Directive EC 95/46 in Member States,* loc. cit.

[79] In contrast, the Spanish Data Protection Authority has considered the processing of biometric data to monitor public and private employees' observance of working hours from a number of angles. It has issued opinions on the matter in a number of reports and in accordance with the LOPD. It takes into consideration "the circumstances of this category of individuals and the difficulty of establishing other procedures which are equally effective and suitable for ensuring compliance with the obligations arising from an employment contract or the statutory relationship binding a civil servant to the Public Administration". Report of 28 February 2006.

[80] Control of access to a school and the monitoring of employees to ensure that working hours are observed bear no resemblance from the legal perspective (in the first case there is a statutory relationship or employment contract and, in the case of the student, the payment of an enrolment fee and the general duty to obtain an education), or from the perspective of a constitutional value, where failure to observe working hours affects service to the public in the Public Administration and a private entrepreneur's management capacity; the truancy of a student, on the other hand, has a much less serious effect on constitutional values.

[81] The CNIL held that access control for a school restaurant based on digital fingerprints would pose too many dangers for misuse and, consequently, was excessive. However, in Avis (2002) the CNIL dealt with biometric access control (contour of the hand) that should be used in school restaurants. The CNIL allowed this technique since it would not

leave ‘traces’ and could not be misused for any other than the original purpose. It is notable that when assessing the legitimacy of data processing, the CNIL focuses mainly on the possibility of using the data for other purposes than those for which it was originally intended and not on the principle of proportionality.

[82] Hence, the use of biometric techniques in school libraries may make children less aware of the risks relating to data protection at an early stage of their lives.