PERSONAL DATA PROTECTION AND CRIMINAL INVESTIGATION

1. INTRODUCTION:

The work of the different police forces involves dealing with a large amount of highly varied data and information. When these data are considered to be of a personal nature, the state security forces have the duty to take into account the rules of criminal law and criminal procedure applicable in each territory or state, as well as the legislation governing the right to the protection of personal data.

This paper sets out to examine the question of whether data protection legislation is in consonance with the police's preventive and investigative function. In other words, we discuss whether the measures introduced to guarantee the right to personal data protection actually contribute to improve the police work in criminal investigation, or if, on the contrary, legislation in this field works against the exercise of this police function.

At this point it is worth clarifying what is meant by criminal investigation and personal data for the purposes of this paper:

- the term criminal investigation refers to establishing the facts of offences that have already been committed and also to the prevention of future crimes. Thus, it should be understood in a broad sense, covering both criminal investigation *stricto sensu* and also what is known as criminal intelligence or information.
- personal data means any information relating to a specific or specifiable natural person. The notion of personal data currently accepted is very broad, covering data or information other than the individual's full name. Thus a person's postal address, telephone number, car registration number, etc., are all considered personal data.

2. OUTLINE OF THE BASIC PRINCIPLES OF PERSONAL DATA PROTECTION LEGISLATION

It should firstly be pointed out that the fundamental principles of personal data protection legislation are virtually identical across all the EU Member States. This is because the domestic laws that govern this field implement European regulatory texts.

Specifically, Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data of 28 January 1981 and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Data protection legislation seeks to guarantee the fundamental right to personal privacy against the risks posed by the information society, i.e. the possibility to accumulate, process and transfer large quantities of personal data easily and massively.
With this aim in mind, and according to the provisions of the above-mentioned EU legislative texts, the following precepts have been laid down as the fundamental principles of personal data protection law:

1- personal data may not be collected or processed without the unambiguous consent of the individual concerned. In this context, the interested or concerned individual will always mean the data subject. This is known as the **principle of consent**. This principle has some exceptions, i.e. cases in which personal data can be collected and processed without the consent of the subject. This is warranted for instance where a law expressly permits unconsented processing, if the personal data are collected and processed by public administrations in the exercise of their authority, etc.

2- any individual requested to provide his or her personal data must be previously informed of the existence and purpose of the file, and of who is responsible for it. **Principle of information.**

3- personal data may only be collected and processed for legitimate, specific purposes. Therefore, they may not be used for any purposes that are incompatible with the purposes for which they were collected. Furthermore, the personal data processed must be adequate and not excessive for the purpose for which they were collected. **Principle of data quality.**

4- once processed, personal data must be cancelled when they are no longer necessary for the purpose for which they were collected, i.e. personal data may not be retained for longer than is strictly necessary. **Principle of retention.**

5- any individual who is the subject of personal data, whether or not he or she is a national of an EU Member State, may request access to such data, i.e. he or she is entitled to be informed of the data concerning him or her that are being processed. Any data subject may also request that his or her personal data be amended or cancelled, and oppose the processing of the data. These are known as rights of **access, amendment, cancellation and opposition**. In Spain, they are also known as "ARCO rights".

6- any processing of personal data, whether or not it is automated, must be protected by the necessary physical and logical security measures to prevent any unauthorised access, alteration, transfer or loss of the data. This is known as the principle of **data security.**

7- lastly, data protection legislation provides that every EU Member State must have an **Independent Supervisory Authority** to ensure that all these principles are complied with. A supervisory authority has been established in all Member States. In Spain, this role is performed by the Spanish Data Protection Agency and the agencies of the different autonomous regions. In Portugal we find the National Commission for Data Protection, in Italy the *Garante*, in France the CNIL, etc.

Having analysed the basic pillars of data protection in Europe, we can now go on to pose the following questions: **Are the different police forces to apply all the principles of data protection legislation listed above when they are engaging in activities aimed at preventing and investigating crime?**
When there is an ongoing police investigation into a crime and/or an individual, is there any sense in saying that the data subject must be informed of the investigation and that the police must obtain his or her consent? Is there any sense in saying that individuals should be able to access (i.e. to gain knowledge of) the data that concern them when they are being investigated in connection with a criminal offence? When do personal data related to a criminal investigation cease to be necessary? Can the police use data collected in connection with a given investigation in a different criminal investigation?

The point in issue therefore is whether personal data protection legislation should be applied to the letter of the law in criminal police inquiries, or whether there should be significant exceptions to the general legal regime.
It is worth pointing out in this respect that, **in Europe**, police processing of personal data was **since the beginning** considered to imply the existence of **an exceptional regime, as was already provided in article 9.2 of Convention 108 of the Council of Europe cited above**.

3. CHANGES IN EUROPEAN DATA PROTECTION LEGISLATION ON POLICE MATTERS

One of the objectives of the European Union is to create a common area of freedom, security and justice. This area, known as the Union's Third Pillar, constitutes the operating ground for police cooperation among the different Member States. It is therefore in this Third Pillar that police forces exchange information and transfer personal data for the purposes of crime prevention and investigation.

The last few years have seen a steady increase in the need for police cooperation with other states, as its role in efficiently countering terrorism and organised crime has come to be regarded as essential.

3.1. Within the Third Pillar, every state has its own criminal and criminal procedural law.

Nevertheless, domestic data protection law is grounded on a common legal substrate formed by the following texts, which offer a picture of legislative progress to date: Convention 108 of the Council of Europe of 28 January 1981 mentioned above, and Recommendation (87) 15 of 17 September 1987 of the Council of Europe regulating the use of personal data in the police sector.

- These legislative texts are applicable to any processing of personal data. Therefore, they are applicable to police data and to any data within the scope of the Third Pillar. Despite having been issued by the Council of Europe, these instruments are applicable in all EU Member States, as they are also members of the Council of Europe. Moreover, these texts have been implemented in the Member States because the Schengen and Europol Conventions so require as a necessary condition.

- These are very general regulatory texts, referring only to personal data that undergoes automated processing. They do not make any provision for the transfer to third party states or institutions.

- The Convention only establishes that personal data processing will be subject to an exceptional regime to the extent that is necessary in a democratic society to guarantee public security and the prosecution of criminal offences.

- The exceptional regime governing police data is detailed in Recommendation (87) 15. It can be summarised as follows:

    a) The text refers to data used for police purposes, defined as those necessary to prevent a real threat to public security or to prosecute criminal offences. In such cases, the police may collect and process personal data without the consent of the individuals concerned. The text does, however, recognise the right of information, provided that it does not hinder the police's investigative activity.
    b) An independent supervisory authority must be established to monitor personal data processing by police forces. This agency will also be informed of all the files used by the police.
    c) Police information must be stored according to its degree of reliability or accuracy. Specifically, a distinction must be made between information based on fact and information based on opinion. A further separation must be established between data for administrative purposes and data for police purposes.

    d) The text makes general provision for data transfer, which is admitted in many different cases at the national and international level.
    e) Provision is made for the principle of purpose, i.e. the police may only use the data for the purpose for which they were collected, unless they are necessary for a specific investigation and subject to the authorisation of the supervisory authority or a legal provision that so permits.

f) The text recognises the rights of access, amendment and cancellation. These may be denied if it is deemed essential for the execution of police duties or necessary for the protection of the data subject or third parties.
g) Compulsory periodical review of the information to determine whether further retention of the data is justified in light of the purpose for which they were collected. This is based on the idea that the need to retain the data must be reassessed at given time intervals.
h) The necessary logical and physical security measures must be put in place.

3.2. The 1990s were marked by the implementation of two international conventions in the area of European police cooperation, each with its own system of information, and both designed to facilitate the exchange of police intelligence: the Schengen Convention and the Europol Convention.
Where data protection is concerned, both these instruments refer to Convention 108 and Recommendation (87) 15 mentioned above.

3.3. The Decisions of the 21st century are characterised in that they aim to step up police cooperation and information exchange among the different European states.

Decision 2007/533/JHA of 12 June 2007, which governs certain police matters, and establishes the so-called SIS II (covering 31 European states, four of which are not part of the EU)**.** This system constitutes a great advancement in certain respects, although it has not yet come into effect. It is expected to enter into force in 2012.

SIS II extends the scope of the previous Convention in that it stresses its declared objective of guaranteeing public security in the European Union and in the territory of its Member States, while also incorporating the exchange of supplementary information in police and judicial cooperation in criminal matters. Thus, what was formerly a system based on guaranteeing the free circulation of people becomes a system for supporting criminal investigation in general.
The fact that it will incorporate linking systems to other SIS II information gives further weight to the argument of its assimilation to a police investigation system.

The regime for personal data protection remains that provided in Convention 108 and Recommendation (87) 15, as Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters will finally only apply to the exchange of data among EU Member States. Schengen and Europol are excluded from its scope of application.

Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office, which entered into force on 1 January 2010 and which replaces the Europol Convention. This Decision effectively leads to Europol's integration in the European institutional framework, although its agents are again devoid of any executive functions.

Its purpose is to step up police cooperation among the Member States by establishing joint investigation teams and improving access to information. It simplifies the

procedure to extend the list of offences over which Europol has competence. No change is introduced as regards the applicable regime in matters of data protection, which is still the acquis of the Council of Europe, i.e. Convention 108 and Recommendation (87) 15.

The principle of availability:

One of the conclusions stated in the **2004 Hague Programme** was that improving the fight against terrorism and organised crime requires implementing the so-called principle of availability, according to which any police officer who needs information to perform his or her duty within EU territory will be able to obtain it from another Member State. In other words, the Programme envisages the **direct exchange of information among Member States, as well as the obligation to share or deliver the information to a requesting state.**

A clear example of this principle is **Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.**

This Framework Decision has been implemented in Spanish legislation through the recently passed Law 31/2010 of 27 July and its complementary Organic Law 6/2010, also of 27 July.

The Framework Decision also refers data protection matters to Convention 108 and Recommendation (87) 15, despite the European authorities' directions to the effect that they should be subject to the regime provided in Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

It should be pointed out that **Council Framework Decision 2008/977/JHA of 27 November 2008** mentioned above was intended to replace Recommendation (87) 15, introducing more specific and up-to-date rules on data protection in the area of police work.
It was designed as a unifying mechanism for data protection within the Third Pillar, in so far as it was to apply to the processing of police information in the individual Member States, and also to the exchange of information among Member States, and between the Member States and other institutions.

But the scope finally given to Framework Decision 2008/977 is extremely narrow, as it only applies to police information exchanges among the Member States, provided that they are not effected through SIS or Europol or that any criminal intelligence is involved. It also applies to transfers to third-party states and to international bodies if the information has been received from another Member State (not when it has been generated by the state making the international transfer of information).

The degree of relevance and effective application achieved by this Framework Decision will therefore depend on whether the Member States take its precepts on board voluntarily when they implement it into their domestic law, or whether they restrict its applicability to exchanges of information between the Member States.

CONCLUSION: The last few years have seen the introduction of mechanisms to facilitate the exchange of police information throughout the EU with the ultimate aim of achieving greater efficiency in the fight against criminality. However, these measures have not been accompanied by new instruments for the protection of personal data to guarantee that such exchanges are fully respectful of individual privacy.
Thus, although these legislative developments have increased police efficiency, no parallel improvement has been seen in the protection of the personal data processed by the different European police forces.

4. THE DATA PROTECTION REGIME OF SPANISH LAW

The files held by the State Security Forces are very briefly provided for in Article 22 of the Organic Law on the Protection of Personal Data 15/1999 of 13 December, which we will hereafter refer to as the OLPPD.

This precept lays down the regime to which police files are subject, differentiating those that have an administrative purpose from those that have a police purpose. Thus, files having an administrative purpose are subject to the ordinary regime established by the OLPPD for personal data processing carried out by the public administration. Files having a police purpose, on the other hand, are subject to a special regime where data protection is concerned.

This distinction is by no means lacking in consequence, as the category of the file determines the legal regime it is subject to.

Significant though this matter is, no definition or idea of what is to be understood by "administrative purposes" and "police purposes" where data protection legislation is concerned is to be found in substantive regulatory texts relating to the police, or in the debates that took place during the passage through Parliament of the Organic Law governing the automated processing of personal data and the OLPPD. [1]

Neither is any definition offered of what is to be understood by the "files of the State Security Forces". One possible definition for police files would be an organised compilation of data, whether it is automated or manual, that has been created to support the management, organisation or activity of the State Security Forces, thus enabling them to perform their statutory functions and duties.

Lastly, it should be noted that the OLPPD itself contains some special provisions in relation to certain State Security Forces files:

- Files established for the investigation of terrorism and serious forms of organised crime are excluded from the scope of the OLPPD with one

[1] Proceedings of Parliament. Plenary Session and Permanent Committee. Year 1991. 4th legislative period. No. 151.
Proceedings of Parliament. Committees. Year 1992. 4th legislative period. No. 425.
Proceedings of the Senate. Year 1992. 4th legislative period. No. 129.
Proceedings of Parliament. Committees. Year 1999. 4th legislative period. No. 744.

exception, as the competent supervisory authority must be informed of the files' existence, general characteristics and purpose prior to their creation (Article 2.2.c) of the OLPPD).

- Files deriving from images and sound recorded by video cameras by the state security forces will be governed in accordance with the specific legislation, and with the provisions of the OLPPD where appropriate (Article 2.3.e) of the OLPPD).