Chapter 5
Biometrics and Data Protection:
These Data Are Derived from an Individual

Francisco Pacheco Andrade
Universidade do Minho, Portugal

Teresa Coelho Moreira
Universidade do Minho, Portugal

ABSTRACT

The special nature of the characteristics used in biometric systems can present privacy challenges that might not arise with traditional identification methods, such as paper documents, because these data are derived from an individual's physical or behavioural features on the basis of a specific procedure, which is partly automated and yields a (reference) template. On account of their nature, these data require special precautions and the respect of the principles related with privacy and data protection.

INTRODUCTION

Ten years ago the world was adjusting to the fact that people could access information in the privacy of their own home from the World Wide Web. Today, technology has taken society to another plateau; people can be tracked wherever they go and whatever they do.

Originally, the word "biometrics" (Alterman, 2003)[1] meant applying mathematical measurements to biology. Nowadays, the term refers to a range of techniques, devices and systems that enable machines to recognize individuals, or confirm or authenticate their identities. Such systems measure and analyze people's physical and behavioral attributes, such as facial features, voice patterns, fingerprints, palm prints, finger and palm vein patterns, structures of the eye, iris or retina, or gait[2].

Biometrics involves techniques used to identify[3] individuals based on a particular trait or physical characteristic unique to that individual or on a behavioral characteristic of an individual[4]. Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies some requirements like universality, distinctiveness, permanence and collectability.

Biometric data are digitized, that is, the data which are recorded are held in digital form and can therefore be subject to detailed computer analysis. Biometrics potentially raises profound privacy implica-

DOI: 10.4018/978-1-5225-0983-7.ch005

tions and a wide and uncontrolled utilization of biometrics raises concerns with regard to the protection of fundamental rights (Alterman, 2003)[5] and freedoms of individuals[6].

Biometric systems record personal information about identifiable individuals[7]. That means their use falls under the provisions of the *Portuguese Data Protection Law, law 67/98, 26 of October and, in the employment relationship under the remit of article 18 from the Portuguese Labor Code.*

Article 2 a) of Directive 95/46/EC defines "personal data" as "any information relating to an identified or identifiable natural person (…) ; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental (…) identity". Also Recital 26 adds the following explanation "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person".

In accordance with this definition, measures of biometric identification or their digital translation in a template form in most cases are personal data. And, one must not forget that some biometric data could be considered sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health[8].

The special nature of the characteristics used in biometric systems can present privacy challenges that might not arise with traditional identification methods, such as paper documents, because these data are derived from an individual's physical or behavioral features on the basis of a specific procedure, which is partly automated and yields a (reference) template. So, the blanket, unrestricted use of biometric data is not permitted. On account of their nature, these data require special precautions and the respect of the principles related with privacy and data protection, especially the principles of legitimacy, proportionality and transparency, because according to Article 6 of Directive 95/46/EC, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In addition, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.

It is also of core importance to pay attention to some privacy-friendly principles when using these data and a previous study of Privacy Impact Assessment and security should also be a primary concern because biometric data are irrevocable.

Biometric data is collected at a starting point, referred to as the time of enrolment. Identities can subsequently be established or authenticated when new data is collected and compared with the stored records.

Using biometric data may only be justified in specific cases by taking account of the relevant purposes and the context in which the data are to be processed[9]. According to the new regulation on electronic identification and trust services for electronic transactions (Regulation EU Nr 910/2014) electronic identification must comply with the principles relating to the protection of personal data provided for in Directive 95/46/EC and authentication for online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. These principles must be applied considering the distinction between physical and behavioral biometrics, and the latter are not necessarily innocuous, since the way someone taps on the laptop, associated with sensoring, may be enough to disclose the identity and build a profile of the user of online services. Furthermore, it must be ensured the compatibility between norms and principles concerning Data Protection and the norms and principles concerning the identification of users in electronic environments. In this regard, the new possibility opened by the Regulation EU Nr 910/2014 on website authentication