Chapter 106
Biometric Data in the EU (Reformed) Data Protection Framework and Border Management:
A Step Forward or an Unsatisfactory Move?

Simone Casiraghi
https://orcid.org/0000-0001-6708-9175
Vrije Universiteit Brussel, Belgium

Alessandra Calvi
Vrije Universiteit Brussel, Belgium

ABSTRACT

Biometrics technologies have been spreading cross-sector in the public and private domains. Their potential intrusiveness, in particular regarding privacy and data protection, has called the European legislators, in the recent EU data protection reform, to introduce a definition of "biometric data," and to grant biometric data specific protection, as a "special category of data." Despite the reformed framework, in the field of border management, the use of biometric data is expected to increase steadily because it is seen as a more efficient and reliable solution. This chapter will look into the reformed data protection and border management legal frameworks to highlight discrepancies between the two, and ultimately assess to what extent the new data protection reformed regime for biometric data is satisfactory.

INTRODUCTION

Biometrics technologies, and the consequent processing of biometric data, have been spreading cross-sector and across Europe in recent years, although the use of fingerprints in criminal and civil matters dates back to the 19th Century (Kindt, 2013). The word "biometrics" originates from the Greek "*bios*"

DOI: 10.4018/978-1-7998-8954-0.ch106

(life) and "*metron*" (measurement) and indicates, roughly, a set of technologies that process biological or behavioral traits for purposes of recognition.[1]

A paradigmatic use case of biometrics in the public sector in Europe is that of border management, where processing biometric data for the identification and the verification of the identity of individuals is portrayed as a more secure, efficient and reliable solution, as it is shown by e.g. the "Smart Border Package" proposed by European Commission (EC) in 2013 and by the revision of the European Union (EU) large-scale information technology systems (IT systems) in the area of asylum and migration. Large-scale IT systems are just one of the many border management instruments to enable and facilitate the exchange of information between authorities within the EU. This is done through, *inter alia*, the processing of different types of biometric data on top of more traditional alphanumeric data (i.e. data represented by letters, digits, special characters, spaces, and punctuation marks).[2]

In recent years, new rules on EU large-scale IT systems were introduced or proposed, and in 2017 the EC proposed to make these information systems interoperable at the EU level. As a result, in early 2019, two regulations for large-scale IT systems interoperability were adopted, one for the EU information systems in the field of borders and visa, and one for the field of police and judicial cooperation, asylum and migration.[3] In both frameworks, biometric data is expected to play a key role, to make these systems "interoperable" by, for instance, creating a common search portal and by establishing a common repository with biographic data of the persons whose data are stored in the different IT system (Fundamental Rights Agency [FRA], 2018, p. 20).

This chapter aims to show the discrepancy between the status of biometric data in these border management instruments and the new status granted to biometric data in the so-called data protection reform package, which includes the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) - other than the Regulation 2018/1725 on the protection of natural persons concerning the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (EUDPR).

The chapter will argue that, despite the efforts to standardize the definition and legal regime of biometric data across the EU, and the safeguards that are in place to protect them in the GDPR, in the LED, and the EUDPR, this is not sufficiently reflected in the case of border management instruments. The main research question will be: to what extent is the new definition and status of biometric data introduced in the reformed data protection framework consistent with the legal framework on the interoperability of EU large-scale IT systems?

The scope of the article is limited to the European Union's data protection framework, although the authors acknowledge the importance of the Council of Europe's instruments for privacy and data protection such as the European Convention of Human Rights and the modernized Convention 108.

To support the argument, the structure will be as follows.

In the next section, the chapter will provide an overview of the reformed EU data protection landscape concerning biometric data. The section will briefly sketch the situation before the entry into force of the GDPR, the LED and the EUDPR, the reasons why the legislator took this initiative (high risks to rights and freedoms of data subjects) and then move to the new definition and the legal status of biometric data in those frameworks.

In the following section, the status of biometric data in border management instruments (i.e. large-scale IT systems and interoperability regulations) will be outlined. Afterward, a short comparison between the GDPR, the LED, and the EUDPR on the one hand and border management instruments, on