Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations

Claire Gayrel *

Senior Researcher at CRIDS (Research Centre in Information, Law and Society), University of Namur, Namur, Belgium

Keywords:
Biometrics
Privacy
Data protection
Proportionality
Necessity
Consent

A B S T R A C T

The Council of Europe recommends promoting proportionality when dealing with biometric data, notably by "1) limiting their evaluation, processing and storage to cases of clear necessity, namely when the gain in security clearly outweighs a possible interference with human rights and if the use of other, less intrusive techniques does not suffice; 2) providing individuals who are unable or unwilling to provide biometric data with alternative methods of identification and verification; (. . .)". France counts as a pioneering Member State in addressing the specific data protection risks raised by the increasing development of biometrics, in particular in the private sector. Since 2004, the French Data Protection Authority, the CNIL, has been empowered to prior check the proportionality of biometric systems deployed in the private sector. It also enforces in practice the articulation between the necessity test and the consent requirement. The present contribution reviews 10 years of CNIL's decisions with respect to biometric systems, then identifies and further discusses the criteria taken into account to apply the necessity test and the consent requirement.

1. Introduction

Biometric technologies are no longer an exclusive prerogative of law enforcement actors, a monopoly of public power. Technological advances in the field and reduction of costs are carrying biometric technologies beyond the fields of forensics, border control and national identification into citizens' everyday life.[1] The special nature of biometric data,[2] notably due to their relative uniqueness, universality and stability,[3] has

* CRIDS (Centre de Recherche en Information, Droit et Société), Faculté de droit, Université de Namur, Rempart de la Vierge 5, B-5000 Namur, Belgium. Tel.: +3281725206; fax: +3281725202.
E-mail address: claire.gayrel@unamur.be.

[1] Under the dir. Ayse Ceyhan & Pierre Piazza, *L'identification biométrique, Champs, acteurs, enjeux et controverses*, Editions de la Maison des sciences de l'homme, Paris, 2011.

[2] We will refer here to the definition provided by the Article 29 Working Party, *Opinion 03/2012 on developments in biometric technologies*, 27 April 2012, WP193, pp. 3–4: "*biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability*".

[3] Nancy Yue Liu, *Bio-Privacy, Privacy Regulations and the Challenge of Biometrics*, Routledge, Abingdon, 2012, pp. 67–68.

http://dx.doi.org/10.1016/j.clsr.2016.01.013

been underlined to advocate for a specific legal protection, whether under special legislation[4] or by extending the definition of sensitive data to include biometric data under general data protection legislation.[5]

The Council of Europe was swift to raise concerns regarding the rapid development of biometric technologies. Already in 2005, the Consultative Committee of the Council of Europe argued for a not too rapid installation of these systems considering that "*an all too enthusiastic rapid introduction may entail unforeseen effects that are hard to reverse*".[6] The Parliamentary Assembly further adopted a resolution calling upon Member States to elaborate a standardized definition of biometric data, revise existing data protection legislations by adjusting them to the specificities of biometric technologies, recommend the use of a biometrics template instead of raw biometrics whenever possible, and promote proportionality in dealing with biometric data, notably by « *1) limiting their evaluation, processing and storage to cases of clear necessity, namely when the gain in security clearly outweighs a possible interference with human rights and if the use of other, less intrusive techniques does not suffice; 2) providing individuals who are unable or unwilling to provide biometric data with alternative methods of identification and verification; (. . .)*"[7] The practical application of this recommendation demands that we articulate the well-known requirements of necessity and of individual consent, both of which progress from European fundamental rights instruments and data protection law.[8] In practice, both requirements may be difficult to articulate when applied to biometric systems deployed in the private sector. Indeed, if a biometric system is clearly necessary, is there any place for individual consent, and thus the possibility to object? Besides, how exactly is the gain in security to be weighed against the interference in individual rights?

By 2014, only a few countries had adopted legislation and regulation specifically aimed at the issue of biometric data and biometric system, among which France counts as a pioneering Member State in the field.[9] Since 2004, the processing of biometric data is specifically foreseen in the Information Technology and Civil Liberties Act.[10] It provides that biometric applications carried out by the State for the identification or verification of identity of individuals must be authorized by Decree after consultation of the CNIL,[11] and that other "*automatic processing comprising biometric data necessary for the verification of an individual's identity*" are submitted to the prior authorization of the CNIL.[12] The CNIL is therefore empowered to apply the principle of proportionality described above, and enforces in practice the articulation between the necessity and consent requirements. All decisions being publicly available, its experience in this field over the last decade affords an interesting case study. The present contribution reviews 10 years of CNIL's deliberations with respect to biometric systems, as well as identifying and discussing the criteria taken into account when applying the necessity test and the consent requirement.

The scope of the present review is limited to the deployment of biometric systems in the private sector, leaving aside the deployment of biometric systems by the State, which are subject to the adoption of a Decree. Instead, we will specifically focus on those situations in which the CNIL is empowered to authorize or refuse the installation of biometric systems which, in practice, broadly speaking covers all biometric identification carried out in the private sector (including public institutions or public services, as long as they cannot be considered as acting in the course of a public State mission). In compliance with the Information Technology and Civil

[4] Els Kindt, *Privacy and Data Protection Issues of Biometric Applications, A Comparative Analysis*, Springer, 2013, in particular pp. 822–829 and chapter 9, "A legal model for the use of biometric data in the private sector", pp. 831–896.

[5] This approach appears to have been retained in the modernization process of European legal data protection instruments, which should provide a specific status to biometric data. See the draft protocol amending the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, CM (2015)40, providing that the processing of "biometric data uniquely identifying a person" shall only be allowed where specific and additional appropriate safeguards are enshrined in law, complementing those of the Convention (art. 6). The draft explanatory report defines the processing of biometric data as those "resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual, which allows the unique identification or authentication of the latter". This definition is more restricted than the one of the Working Party 29 (see footnote 2) since it excludes behavioural characteristics, such as gait analysis.

[6] Consultative Committee on the Convention for the protection of Individuals with regard to the automatic processing of personal data (T-PD), Progress Report on the application of the principle of Convention 108 to the collection and processing of biometric data (2005), p. 8. In a landmark case, the Court of Strasbourg also raised concerns regarding the possible future uses, yet unknown, of biometric data and gave strong weight to this argument to qualify the collection of DNA data as an interference into individuals' rights under Article 8 of the ECHR in its judgement *S. and Marper v. the United Kingdom*, 4 December 2008.

[7] Council of Europe Parliamentary Assembly, Resolution 1797 (2011) on the need for a global consideration of the human rights implications of biometrics of 11 March 2011.

[8] In particular, the requirement of necessity to justify interferences into individuals' right to private life is provided in Article 8 of the European Convention of Human Rights (ECHR) and Articles 7 & 52§1 of the EU Charter of Fundamental Rights. The requirement of consent is now enshrined in Article 8 of the EU Charter. See also article 7 a) of 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, OJEC L 281, 23 November 1995.

[9] Paul de Hert & Koen Christianen, *Council of Europe Progress Report on the application of the principles of convention 108 to the collection and processing of biometric data*, January 2014.

[10] Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties – Loi No. 78-17 Informatique et Libertés du 6 Janvier 1978 – as amended, available here: http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (last accessed 1/11/2015).

[11] Article 27§2 of the Information Technology and Civil Liberties Act.

[12] Article 25§8 of the Information Technology and Civil Liberties Act.