The principle of proportionality applied to biometricss in France

Gayrel, Claire

Published in:
Computer Law and Security Review

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

COMPUTER LAW & SECURITY REVIEW ■■ (2016) ■■–■■

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

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 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).

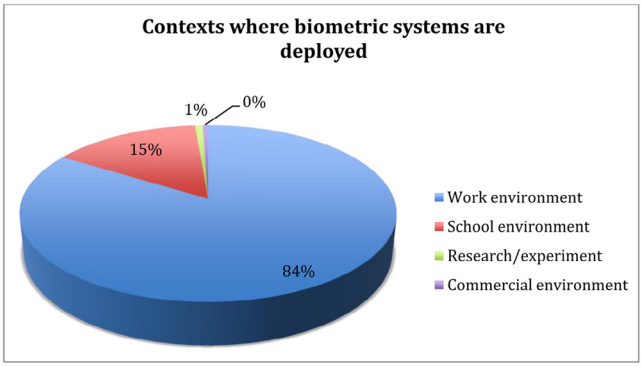
[11] Article 27§2 of the Information Technology and Civil Liberties Act.

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

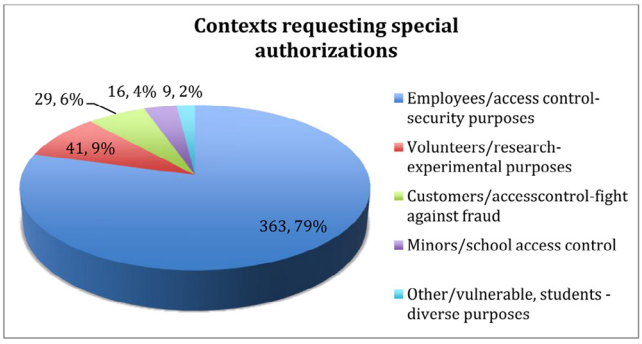
Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

Liberties Act, the CNIL has adopted unique authorizations[13] regarding a limited processing list for biometric data, now submitted to a simplified declaration: Decision AU-007 on the use of hand geometry to control access to work premises and mass catering[14]; Decision AU-008 on the use of fingerprinting exclusively stored in a personal device to control access to professional premises[15]; Decision AU-009 regarding the use of hand geometry to control access to school restaurants[16]; Decision AU-019 on the use of vein pattern recognition to control access to professional premises[17]; Decision AU-027 on the use of fingerprinting in professional laptops.[18] All other processing procedures remain subject to prior examination and authorization of the CNIL.

In total, about 4850 biometric systems have been notified to the CNIL between 2005 and 2014.[19] About 4400 concern simple declarations and 458 special decisions, among which 101 systems have been refused, an average of about 2% only. The work environment is indisputably the context where biometrics is the most prevalent (≈84% of biometric systems),[20] followed by schools (≈15%),[21] and the use of biometrics for research or experimental purposes (≈1%). The use of biometrics in commercial environment or for other purposes represents less than 1% of biometric systems in France.



We have conducted a thorough analysis of 458 deliberations (comprising both authorizations and refusals) of the CNIL, delivered in compliance with its power of special authorization within the decade from 2005 to 2014.[22] The proportion of special deliberations relating to these different contexts and uses also confirms that employers are those who most request special authorizations (363 special decisions), followed by the research field (41 decisions) and service providers/commercial premises (29 decisions). Only a few deliberations relate to schools (16 decisions), showing that other uses of biometrics outside the conditions authorized by AU-009 are undeveloped. Finally, a small number of decisions (9 decisions) relate to other contexts or categories of individuals, including students or vulnerable people.



[13] Article 24 of the Information Technology and Civil Liberties Act.
[14] Unique Authorization AU-007 – Deliberation n°322–2012 of 20 September 2012.
[15] Unique Authorization, AU-008 – Deliberation n°102–2006 of 27 April 2006.
[16] Unique Authorization, AU-009 – Deliberation n°103–2006 of 27 April 2006.
[17] Unique Authorization, AU-019 – Deliberation n°316–2009 of 7 May 2009.
[18] Unique Authorization, AU-027 – Deliberation n°074–2011 of 10 March 2011.
[19] This figure derives from the figures published by the CNIL in its Annual Reports over the period 2005–2014 and from the Report of Senator François Pillet to the Senate of 16 April 2014, available here: http://www.senat.fr/rap/l13-465/l13-4651.pdf (last accessed 1/11/2015).
[20] The proportion of biometric systems in the work environment is estimated on the basis of the number of simple declarations (All declarations relate to the work environment except AU-009) and special deliberations (special authorizations and refusals) concerning the enrolment of employees.
[21] In its 2010 Annual Report, the CNIL mentions that about 400 biometric systems have been notified to the CNIL in accordance with the Authorisation unique AU-009 (adopted in 2006) for access control to school catering, an average of 100 declarations per year. No other figures have been published further. For the purpose of our estimation, we have raised this number up to 800 (following the average of 100 declarations per year). See CNIL's Annual Report 2010, p. 31 here: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_rapport_annuel_%202010.pdf (last accessed 1/11/2015).

[22] All these deliberations have been classified according to some pre-defined essential context-related information and characteristics of the systems: i) date of the decision; ii) authorization or refusal; iii) activity of the requesting entity (such as "laboratory", "casino", "hospital/health establishment", "industry/fabrics", "other private firms", "firms in the field of surveillance/security technology", "association", "school establishment", "banking/financial sector", "research", "experience", and "other"); iv) categories of people enrolled in the system ("minors", "employees/habilitated persons", "customers/users of public services", "patients", "volunteers", "vulnerable people", "students", "other"; v) type of system ("simple" or "multimodal"); vi) type of biometric characteristics collected ("fingerprint", "finger vein", "palm vein", "hand geometry", "iris", "voice", "DNA", "face recognition"); vii) purposes pursued ("identity fraud", "general security", "access control to applications/devices/", "access control to restricted area", "other"); viii) legal basis invoked ("consent", legitimate interests of the controller"); ix) place of storage of the biometric data ("individual device", "terminal/reader", "central storage/server")/.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

We will now analyse in more detail the requirements applied by the CNIL and the concrete situations in which biometrics was deemed (or not) proportionate within the work environment (2), the school environment (3), the commercial environment (4), in the research field (5) and in residual cases (6). Finally, we will see how CNIL's policy is being reconsidered (7).

2. Biometrics in the work environment

79% (364) of CNIL's deliberations concern the enrolment of employees in biometric systems, among which a proportion of three-quarters have been authorized (272 authorizations for 92 refusals). The work environment is indisputably the context where biometrics is presently the most expanded and employers are those who are the most requesting special authorizations for biometric systems to the CNIL. Such systems are deemed necessary for a variety of purposes: access control to specific restricted areas (≈33%), general security of the work area/premises (≈28%), access control to professional applications, devices or network (≈21%), control of the working time of employees (≈14%) and other uses (demonstration, exhibition, other . . . about 3%).

CNIL's policy with respect to biometrics in the work environment requires that the use of biometrics for working time management purposes be distinguished (1) from the use of biometrics for security-related purposes, which represents the majority of biometric uses. Within this category, one must further distinguish the use of biometrics in situations of "pressing security need" (2) and the use of biometrics for general security purposes (3).

2.1. *The management of working time*

CNIL's position regarding the use of biometrics for controlling the working time of employees has evolved substantially in the last decade, from a careful authorization of the use of hand geometry, towards a general prohibition of the use of any biometrics for such purposes.

The use of biometric systems to manage employees' working time was one of the first uses to be submitted to the CNIL for prior consultation. In 1999, the CNIL delivered an opinion regarding the use of such systems by a local prefecture and the national airport Roissy-Charles de Gaulle. In both cases, the systems relied on the use of fingerprint, and the CNIL concluded that the collection of such biometric data was disproportionate.[23] In its 2001 activity report, the CNIL provided a summary of its doctrine regarding biometrics, relying on the distinction between biometric data *leaving trace* and biometric data *leaving no trace*. The CNIL explained that fingerprint or DNA, contrary to some other biometric characteristics, can be collected and exploited without the individual's knowledge and are susceptible to further exploitation for incompatible purposes.[24] In 2001, the CNIL lists the iris, voice and hand geometry as biometric data leaving no trace, nevertheless highlighting the possibility of revising this list in the light of technological advances.[25]

After a series of refusals,[26] the CNIL eventually authorized a biometric system based on hand geometry[27] and further adopted the unique authorization AU-007 regarding the use of hand geometry for work-time management of employees and access control to professional premises.[28] The recourse to hand geometry, a biometric characteristic that was deemed "without trace", was then considered less problematic than fingerprint and therefore considered *a priori* proportionate.

However, the CNIL reviewed its position in 2012 and excluded the purpose of work-time management from the scope of the unique authorization AU-007.[29] This reversal of opinion is remarkable and appears to arise from resistance among labour unions to the generalization of biometrics in this extremely sensitive area of the relationship between employees and their employers. After 2006, the CNIL organized a consultation among relevant stakeholders, in particular labour unions, employers' associations and other professionals in France. According to the CNIL, the outcome of the consultation demonstrated a consensus among them against the use of biometric systems for time control and time management of employees. The main reason put forward is that biometric systems would negatively impact the traditional relationship of confidence between employers and employees, with the risk that this could damage the social climate.[30] Where time control and time management of employees are deemed necessary, the stakeholders considered traditional systems (without biometrics) to be sufficient. Use of biometrics for such purposes, regardless of the biometric characteristic, is now considered *a priori* disproportionate. Several authorization requests have since been submitted to the CNIL (24 requests in 2013 and 5 in 2014), but these have systematically been rejected. This prohibition of biometrics in the employment context is interesting, as it shows that applying the proportionality principle to biometrics does not only rely on the characteristics of the system (type of data, type of storage, function of the system *etc.*), but remains primarily dominated by contextual and cultural aspects that concern its objectives and its environment.

[23] Deliberation n°057-00 of 16 November 2000, opinion about the use of fingerprint for the purposes of controlling the working time of employees by the Prefecture of Hérault. See also CNIL's annual report 2000, pp. 111–113.

[24] CNIL's annual report 2001, p. 171, available here: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000377.pdf (last accessed 1/11/2015).

[25] *Idem*.

[26] Deliberation n°031–2005, n°034–2005, n°035–2005, n°036–2005, n°037–2005 of 17 February 2005, all refusing the use of fingerprint for working time management purposes.

[27] Deliberation n°135–2005 of 14 June 2005 authorizing the Hospital Centre of Hyères to use hand geometry for controlling the working time of employees.

[28] Deliberation n°101–2006 of 27 April 2006, Unique authorization AU-007 regarding the use of hand geometry for access control to professional premises, catering and working time management of employees.

[29] Deliberation n°322–2012 of 20 September 2012 modifying the unique authorization AU-007.

[30] *Idem*.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

2.2. *Situations of "pressing security need"*

Besides the monitoring of working time, biometric systems are widely used for security reasons in the work environment. For certain types of systems, the CNIL normally requires a "pressing security need". The criterion of the existence of a "pressing security need" is indeed essential in CNIL's policy, when evaluating the necessity of storing biometric data that either *leaves a trace* or presents a *high level of accuracy* within a central database, or with a view to identifying individuals.

The CNIL considers that "*the constitution of a fingerprint database can only be admitted in particular circumstances where the identification of individuals is required by a pressing security need*".[31] In such cases, the collection and central storage of biometric data leaving trace, in particular fingerprints can be justified in view of identifying individuals. The CNIL elaborated this issue earlier[32] and has consistently recalled this doctrine in its deliberations. Cases of "pressing security need" have further been interpreted as situations where a biometric system aims at controlling access to a "*delineated area*" representing a "*major stake, which surpasses the strict interest of the organization*".[33] In those cases, the CNIL authorizes the use of fingerprints, alone or combined with another biometric characteristic, and their central storage (in a reader or in a central server). These systems are usually considered more intrusive into individual's rights to privacy and data protection than the storage of the biometric characteristic in an individual device. The issue of storage in the field of biometrics is crucial for the security of the biometric data. Indeed, centralized storage of biometric characteristics, even in the form of templates, presents higher levels of risk in case of accidental loss, alteration, unauthorized disclosure or access.[34]

Moreover, although it is not made clear in CNIL's deliberations, biometric systems that are justified on the ground of a "*pressing security need*" appear to rely on a functionality of *identification*, which must be distinguished from the functionality of *verification* of biometrics.[35] A *verification* system is the process of comparing the biometric data of an individual acquired at the time of the matching with one single biometric template (referred to as a 1:1 matching process). The biometric data may be stored in an individual device[36] or in a central database.[37]

In contrast, a system of *identification* involves the comparison of biometric data with a number of previously stored biometric templates (referred to as a 1:n matching process). Such systems necessarily involve the centralized storage of biometric characteristics, although certain security measures may be applied to prevent unauthorized access, but they also present higher risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.[38]

We will now see how the requirements of a "*delineated area*" and of a "*major stake, which surpasses the strict interest of the organization*" have been interpreted in certain concrete situations by the CNIL.

2.2.1. *The delimitation of a specific restricted area*

Certain restricted areas of a given place may require the installation of a biometric gate to filter access to particular rooms. Such systems have been authorized by the CNIL regarding access control to the strong room of a casino by a limited number of designated employees, for example.[39] The CNIL also authorized the deployment of a comparable system to control access to the operating rooms of a Hospital Centre subject to unauthorized intrusions.[40] However, the CNIL rejected a comparable system that was not limited to operating rooms, but extended to the recovery room, cloakrooms and other areas of the hospital since the system appeared to respond to a "general security" objective and was not limited to a restricted area.[41]

2.2.2. *The requirement of a "major stake which surpasses the strict interest of the organization"*

The requirement of a "*major stake, which surpasses the strict interest of the organization*" is of course decisive in the policy of the CNIL with respect to the central storage of fingerprints. For example, the storage of fingerprints in a centralized server has been authorized with the intention of identifying employees permitted to access a SEVESO-classified[42] chemical plant, controlling access to the Satellite Control Centre,[43] to the National

[31] CNIL's Communication regarding central storage of fingerprint of 2007, available here: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf (last accessed 1/11/2015).

[32] See for example deliberation n°023–2005 of 17 February 2005 authorizing the French Central Bank to deploy a biometric system to control access of employees to sensitive areas.

[33] See deliberation n°254–2007 of 13 September 2007 refusing the deployment of a biometric system relying on the verification of fingerprint by the society Ecureuil Lease.

[34] Els Kindt, *op. cit.*, pp. 353–363.

[35] See the definition and implications of verification systems and identification systems in Opinion 3/2012 of Article 29 Working Party on developments in biometric technologies of 27 April 2012, WP193, pp. 5–6.

[36] The biometric data may be stored in a personal device, as a laptop, or on a token or a badge belonging to the data subject.

[37] The centralized storage may be preferred by data controllers when the use of a badge or a token is proved inappropriate in given circumstances (e.g. risks of loss). In this case, the data subject is generally active in order to extract the biometric template from the central database prior to the matching. Most frequently, the extraction/selection of the template in carried out through a PIN code known exclusively by the data subject.

[38] See Els Kindt, op. cit., pp. 647–654.

[39] Deliberation n°088–2007 and n°092–2008 authorizing the central storage of fingerprint by the Casinos of Nivernais and La Baule to control access to the strongroom.

[40] Deliberation n°080–2007 of 25 April 2007 authorizing the Hospital of Strasbourg to deploy a biometric system relying on fingerprint to control access to operation rooms.

[41] Deliberation n°328–2008 of 11 September 2008 refusing the deployment of a biometric system relying on fingerprint to control access to certain areas of the "association hospitalière de l'Ouest".

[42] Deliberation n°051–2007 of 21 March 2007 authorizing Millennium Chemicals Thann SAS to deploy a fingerprint biometric system to access to sensitive areas of the chemical plant and deliberation n°2011-280 of 21 September 2011 authorizing TRAFICTIR Rhone-Alpes to deploy a fingerprint biometric system to control access to the site.

[43] Deliberation n°464–2010 of 9 December 2010 authorizing EUTELSAT SA to deploy a fingerprint biometric system to control access to the satellite control posts.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

Printing office where ID cards and passports are printed,[44] to control access to government servers containing large amount of personal data,[45] or to control access to premises where classified/confidential information is stored.[46] In contrast, the CNIL has rejected a comparable system intended to control the access of employees to the offices of the CEO of a CAC 40 company.[47] According to the CNIL, "*nothing demonstrates that the potential intrusion of unauthorized persons would threaten the protection of goods or people essential to the collectivity*." It further adds that "*the sole fact of being the CEO of a CAC 40 company does not in itself justify recourse to a central fingerprint database*." It is one of the rare decisions where the CNIL provides some further interpretation of the criterion of a "*major stake*" referring to the "*protection of goods or people essential to the collectivity*".

The storage of fingerprints in a terminal/reader, not connected to any network, seems more acceptable to the CNIL. Many decisions nevertheless lack contextual information about the activities of the organizations requesting authorizations for a biometric system. It is therefore difficult to evaluate the relevance of the security needs invoked. For example, in two decisions of the same day, the CNIL reached two opposite conclusions regarding access control to computer rooms. On the one hand, it rejected a biometric system based on the storage of fingerprints in a reader to control access to the servers of a data processing centre, although the activity of the company is related to the processing and storage of a large amount of data.[48] In this first decision, the CNIL recalls its doctrine and notices that the requesting organization failed to prove a "*major stake, which surpasses the strict interest of the organization*." On the other hand, the CNIL authorized the use of a comparable system to control access to an SME's server specialized in biometric systems. In this decision, the CNIL avoids invoking the criterion of a "*major stake*" and apparently justifies its decision on technical security grounds (the adoption of strong security measures to protect the biometric templates stored in the reader).[49] In this decision, the criterion of a "*major stake*" is simply put aside, and not even discussed. In our view, the activity of the company (producing biometric systems) can hardly qualify as a "*major stake, which surpasses the interests of the organization*". It is rather unfortunate that the CNIL abandoned this criterion in this particular case and judged the system admissible on technical security grounds only.

2.3. *General security objective*

When the organization fails to demonstrate a "pressing security need" and instead pursues a general or vague objective of security of its premises and/or devices, the CNIL admits the use of two alternative types of biometric systems. First, the CNIL recommends the recourse to *verification* systems (see *supra* the distinction with identification systems) with a storage of the biometric characteristic in an individual device exclusively held by the data subject, which presents less risks in case of loss or attack. Biometric access controls to professional computers and applications are systematically authorized by the CNIL, whatever the biometric characteristics (with trace or not) if these are stored in an individual device.[50] According to the CNIL, such systems do not present any specific risk for the individual's rights to privacy and data protection.[51] Second, if tokens or badges are considered inappropriate in certain circumstances, the CNIL favours the recourse to biometric data leaving no trace. In particular, systems relying on hand geometry, hand/finger vein recognition and iris scans (which are considered as leaving no trace by the CNIL), have been authorized in the professional context, even when stored centrally.[52] Again, we can see that beyond the functionality of the system (verification or identification) and type of storage (centralized or not), the type of biometric data has been of particular importance in the decision to authorize or refuse the use of biometrics for general security objectives.

3. Biometrics in the school environment

The use of biometrics in the school environment, in particular to access school catering has been generalized in the 2000's. The enrolment of minors in the school environment is the second major context of deployment of biometric systems in France. Hundreds of biometric systems have been installed in secondary and high schools in order to control and manage access to school catering. In this context, instead of security-related motivations, the deployment of biometrics appears to be commanded by an imperative of management.[53] In 2005 and 2006, the CNIL indeed authorized the use of hand geometry to control access to school catering and further adopted the unique authorization AU-009. The system is supposed to limit identity fraud and facilitate the issuing of invoices. Since then, only three special decisions relate to other biometric uses in

[44] Deliberation n°113–2005 of 7 June 2005 authorizing the National Printing Office to deploy a fingerprint biometric system to control access to the places where ID cards and passports are produced.

[45] Deliberation n°256–2007 of 13 September 2007 authorizing the Inter-Regional Centre of Information Processing of Lyon to deploy a fingerprint biometric system to control access to certain restricted areas, where servers of the public administration are located.

[46] Deliberation n°223–2011 of 21 July 2011 authorizing the society Compagnie Européenne d'Intelligence Stratégique to deploy a fingerprint biometric system to control access to restricted areas where sensitive files with high level of classification are stored.

[47] Deliberation n°056–2008 of 6 March 2008 refusing GIE 32 Hoche to deploy a fingerprint biometric system to control access to the offices of the CEO of Bouygues SA.

[48] Deliberation n°257–2011 of 21 September 2011 refusing the installation of a biometric system based on fingerprint by the data processing Centre GROUPE MIT. See also a decision where the CNIL rejected a comparable system to control access to the computer room of a society developing gambling software, deliberation n°185–2011 of 23 June 2011.

[49] Deliberation n°282–2011 of 21 September 2011 authorizing the installation of a biometric system based on fingerprint by the society BE METRICS.

[50] We count 59 authorizations and none refusal.

[51] See CNIL's Annual Activity report 2001, p. 171.

[52] We count 103 authorizations of use of hand geometry and finger/palm vein recognition systems with a central storage in the reader or in server in the professional context and none refusal.

[53] Xavier Guchet, « La biométrie à l'école : une approche anthropologique », in *L'identification biométrique, Champs, acteurs, enjeux et controverses*, *op. cit.*, pp. 161–176.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

the school environment, which have all been rejected by the CNIL. Hereunder we will comment three major findings regarding CNIL's approach to biometrics in the school environment.

3.1. *Type of biometric characteristic and type of system*

In 2011, the CNIL rejected the use of finger vein recognition to control access to school restaurants, considering that this biometric characteristic was more intrusive than hand geometry.[54] According to the CNIL, although finger vein is presently a biometric technology that does not leave a trace, alongside hand geometry, finger vein constitutes a more accurate biometric characteristic, and its use should be strictly limited regarding minors. The recourse to finger vein for the purposes of controlling access to school restaurants was therefore considered disproportionate. The intrusive character of the biometric system is also evaluated according to the accuracy of the biometric characteristic. The more accurate and stable the biometric characteristic the more intrusive will be the system, notably with respect to minors whose biometric characteristics may not be definitive and are subject to evolution. Whereas in other contexts, the efficiency of biometric systems (often correlated to the level of accuracy of biometrics) is generally one of the core reasons invoked for justifying the use of biometric data, this argument is actually irrelevant in the case of minors. Indeed, because of their age, the CNIL prefers the recourse to biometric data that will be less stable in time and subject to change.

Besides, the CNIL provides that the biometric system shall be associated with a personal identification code in order to be activated, so that the system relies on a functionality of verification (1:1 matching).[55] In this case, the CNIL authorizes the central storage of the hand geometry in the reader, but requires the individuals to enter a PIN code in order to proceed to the matching. Surprisingly, the CNIL does not explicitly address the possibility of storing the biometric template in an individual badge. We suppose that the central storage of the biometric templates in the reader, instead of a decentralized storage, is motivated by the fact that badges would prove inappropriate due to frequent loss or pupils' failure to carry them.

3.2. *The use of biometrics for security-related purposes is disproportionate*

The CNIL has rejected the deployment of biometric systems for security-related purposes, such as the use of fingerprint to control pupil access to school premises[56] or the use of finger vein to control access to the luggage storage.[57] In both decisions, the CNIL emphasizes the intrusive character of the biometric characteristics chosen, respectively fingerprint and finger vein and the type of system envisaged (centralized storage of biometric data). But most importantly, it is the purpose for which the biometric system is envisaged that appears problematic for the CNIL. In both cases, the CNIL considers that the security-related purposes pursued could be achieved through *non-biometric solutions*. It therefore appears clearly that the CNIL is not willing to authorize biometric systems for such purposes in schools.

3.3. *Consent as the legitimate basis*

In its unique authorization AU-009 regarding the use of hand geometry to control access to school restaurants, the CNIL provides that individuals must be properly informed about the processing of their biometric information and explicitly consent to be enrolled in the system.[58] A minor individual and his/her parents or legal representative must consent. Their right to object to the processing of their biometric information shall be respected and alternative means to control access be implemented. The requirement of the individual's consent, as provided by article 7 a) of the directive 95/46, follows from the purposes of the biometric system, which are related to a general goal of identity management in order to grant access to the catering, fight against identity fraud and facilitate billing administration. Contrary to the use of biometric data in the professional context, where "*legitimate interests*" of security are invoked, here the goal of identity management is overridden by the legitimate interests of fundamental rights and freedoms of individuals arising from article 7 f) of the same directive.

4. Biometrics in the commercial environment

Only 29 decisions deal with the enrolment of customers in biometric systems to access commercial services, among which 3 have been rejected by the CNIL. Although few in number, each deliberation is especially enlightening as to the conditions under which biometrics may expand in everyday life in the future (see also section 7.1).

4.1. *The condition of storage in an individual device*

In the context of the commercial environment, it is the type of storage rather than the biometric characteristic, which proves to be decisive. The CNIL strictly applies the requirement of a decentralized storage in an individual device.

This requirement has been applied to casinos where biometric systems have been widely deployed as a means to speed-up access control at the entrance. The installation of biometric

[54] Deliberation n°147–2011 of 19 May 2011 refusing the College ATURRI to deploy a finger vein biometric system in order to control access to the catering.

[55] Unique Authorization AU-009 of 27 April 2006, article 5.

[56] Deliberation n°178–2008 of 26 June 2008 refusing the high school of Boulogne-Le Portel to deploy a fingerprint biometric system to control access to the establishment. The system was in particular intended to prevent unauthorized people from accessing the premises, preventing pupils below the age of 16 to leave the school without prior authorization and fight against school absenteeism.

[57] Deliberation n°388–2011 of 1 December 2011 refusing the high school LES IRIS to use finger vein recognition to control access to the luggage storage.

[58] Unique Authorization AU-009 of 27 April 2006, article 6.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

systems followed from a modified legislation,[59] providing that casinos had to put in place strict identity controls to check whether their customers are allowed access to gambling establishments. Indeed, gambling establishments are forbidden to minors and any individuals included in a black list maintained by the Ministry of Homeland Security.[60] The entrance into force of the decree resulted in a substantial increase in the identification processing time per customer. In order to increase the efficiency of identity checks, casinos sought to deploy biometric verification systems to speed-up this process for prevetted frequent customers. The CNIL authorized the enrolment of frequent customers for the purpose of the verification (1:1 matching) of their identity, with a storage of the biometric information as a template and in an individual device (card) exclusively under the control of customers.[61] However, the CNIL rejected the deployment of a biometric identification system (1:n matching), where the biometric information was stored in a centralized server, considering the interference into individual's rights disproportionate.[62]

Apart from casinos, four special authorizations concern the deployment of biometric verification systems in recreational spaces (e.g. sports facilities) with a view to verifying customer identity and combating identity fraud, judged prejudicial to the economic benefit of the owners.[63] In all cases, the biometric information is stored on an individual device exclusively held by the data subjects. In contrast, the CNIL rejected the deployment of a biometric system in hotels intended to identify customers, mainly because the proposed system relied on the centralized storage of biometric information and a system of identification. Instead it suggests that biometric templates should be stored in an individual device under the control of individuals.[64]

The decentralized storage of the biometric information on an individual device held exclusively by the data subject appears to be a strict condition for the biometric identity control of customers. Considering that biometric access control to commercial services relies much on convenience motivations and not on reasons of strict necessity, it is legitimate to require the system's characteristics to present the least level of data protection risk possible.

4.2. *Consent as the legitimate basis*

As in the case of schools, the enrolment of customers in biometric systems is not compulsory and can only be carried out on a voluntary basis. Customers must be provided with an alternative non-biometric identity control procedure and cannot be enrolled without their explicit and specific consent. The legitimate interests of the controllers, such as the fight against identity fraud for the economic well-being of the firm, are in no wise considered sufficient to override the individual's rights and freedoms. As a consequence, and in compliance with data protection legislation, the legitimate basis of such systems must rely on the individual's consent to enrol in the system.

5. Biometrics for research or experimental purposes

Biometric systems deployed for purposes of research or experiment constitute the third most important use for which controllers are requesting special authorizations to the CNIL. Over the 41 relevant decisions, all biometric systems have been authorized by the CNIL, and only in exceptional cases has the CNIL restricted the scope of the experiment.[65] Two types of decisions can be distinguished: those relating to research purposes and those requested for real experimentation of biometric systems, which are therefore deployed in real conditions. This second category is very relevant since it shows potential future uses of biometrics presently at the experimental stage that could be widely deployed in a mid-term perspective. In all cases, individuals are enrolled on a voluntary basis, and their consent therefore legitimizes processing.

The CNIL showed itself to be very open to research and experience in the field of biometrics. Firms in the security and surveillance sector request authorizations for field trials of new biometric access control systems.[66] One authorization related to the use of thermal information for the improvement of the interface between the on-board computer and the driver in the auto industry.[67] 11 special authorizations have been delivered in the banking sector. Most of them relate to experimentation with biometric authentication of customers in order to increase the security of contactless payments.[68] In this case, the biometric characteristic is stored in the card and used to authenticate the customer instead of the traditional PIN code. CNIL's deliberations also relate to experimentation with voice authentication of customers for phone-banking services, again

[59] Decree n°59–1489 of 22 December 1959 regulating gambling places and casinos as modified by Decree 2006-1595 of 13 December 2006.

[60] While individuals can voluntarily ask to be registered in the blacklist, some are registered following an administrative exclusion.

[61] See for instance, deliberation n°146–2007 of 21 June 2007 authorizing the use of fingerprint to control access to the Casino of Cap d'Agde.

[62] Deliberation n°131–2010 of 20 May 2010 refusing the Casino Royal Concorde to use fingerprint to control access to the casino.

[63] See notably deliberation n°138–2007 of 21 June 2007 and deliberation n°196–2013 of 11 July 2013.

[64] Deliberation n°526–2009 of 24 September 2009 refusing the Society APPIA to install a fingerprint biometric system to control access to the hotel.

[65] See for example, deliberation n°423–2011 of 15 December 2011 about the research project SAIMSI aiming at the automatic identification of a speaker or an author of a text. The consortium involved the French Ministry of Defence and Ministry of Homeland Security and the overall goal was to increase the automatic identification of authorship of some online content.

[66] See for instance deliberation n°84–2008 of 27 March 2008 for the experimentation of a mobile biometric identification device.

[67] Deliberation n°264–2014 of 26 June 2014.

[68] See for instance, deliberation n°039–2012 of 2 December 2012 regarding the experimentation of a contactless payment means with multimodal biometric system (fingerprint and finger vein recognition).

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

as a means to increase the security of communications and transactions.[69]

Besides these, one of the most remarkable experiments relates to the real world trial of a biometric system for the identification of patients by the Centre Oscar Lambret, a hospital radiotherapy service.[70] More specifically, two consecutive authorizations have been issued, each one for a one-year trial period. These trials are of particular interest given the potential of biometrics in monitoring identity in hospitals and the healthcare system in general. Indeed, identity monitoring in the hospital context refers to the management of identity and risks of error in the identification of patients, which exists in all hospitals and has a potential to cause accidents, and which require the deployment of procedures and monitoring systems to avoid such accidents.[71] The trial was carried out in a radiotherapy service, where patients are generally treated several times a week during several weeks (an average of 5 sessions a week during 4 to 7 weeks).[72] The Center treats an average of 300 patients per day and carries out about 30,000 sessions of radiotherapy per year. Multiple health actors are involved and work on a just-in-time basis. Accurate identification of patients is a high priority and it is not surprising that the efficiency of biometric technologies may be tested in such a context.

The first authorization concerned the storage of fingerprints in a central database for the purposes of the identification (1:n matching) of the patient. The use of fingerprint was preferred to the use of finger vein by considering scientific studies demonstrating that finger vein could significantly be altered as a consequence of chemotherapy treatment (often combined with radiotherapy). Moreover, the decentralized storage of the biometric characteristic (e.g. in a smart card) was discarded due to risk of loss or forgetfulness. The decision makes clear that the biometric technology is used in support of the organization of the service and can in no case take the place of the final human checking. In practice, the person operating the computers and machine is responsible for a final check of a patient's identity before launching the session. The results of the first year of experimentation showed that 17 false identifications occurred for 28,391 sessions and that accidents were avoided thanks to the systematic human checking.[73] Although the system was deemed well-accepted among the patients, the use of fingerprint proved inappropriate for 5% of patients. According to the CNIL, the interest of biometric technologies in terms of public health is therefore not demonstrated.[74] The CNIL nevertheless authorized a second one-year trial, aiming at increasing the accuracy of the system with a combination of both fingerprint and finger vein. However, it rejected the extension of the experiment to hospitalized minors below the age of 15. Although biometrics can be very promising for identity monitoring in the hospital context, it follows from the CNIL's decision, that the legitimacy of biometrics in such a context relies heavily on its efficiency in eliminating false identification of patients. As the CNIL reminds us, a comparative evaluation of non-biometric identification and its associated risks and accidents with biometric identification of patients still needs to be carried out.[75]

6. Other uses

There are a number of other decisions concerning the installation of biometric systems in other contexts. Although they represent a small minority, they are nevertheless particularly interesting as they enlighten us as to possible further contexts for the use of biometrics. We will comment in this section the enrolment of vulnerable people in biometric systems on the one hand and the use of biometric data to identify candidates to an exam on the other.

6.1. *Biometrics systems and vulnerable people*

In 2008, the CNIL authorized the use of a biometric system to control access to a social accommodation and rehabilitation centre to prevent unauthorized access.[76] The fingerprint template is stored on a personal badge, but most importantly the individuals hosted in the Centre are provided with the choice to refuse the system. In a comparable context of access control to a community home of young workers, the CNIL rejected the installation of a biometric system on the ground that individuals were not provided with the choice of whether or not to be enrolled in the system.[77] In a particularly interesting third decision, the CNIL authorized an identification system (1: n matching) relying on the central storage of finger vein data to control the presence of mentally disabled persons at work.[78] The goal of the system is to control the presence of employees in the bus driving them to their work and at the work premises in order to signal any absence to their family or legal representative and thereby facilitate potential searches. In brief, the system intends to "*offer more autonomy to mentally disabled persons while guaranteeing their security*".[79] A system of identification with central storage of the biometric data is justified because badges proved inappropriate due to recurrent loss or failure to carry and inability of the persons concerned to memorize a PIN code. In this context, it is stated that the system satisfies the condition of proportionality, in particular because

[69] See deliberation n°375–2014 of 25 September 2014 for the experimentation of a system "talk to pay" (voice recognition of customers).

[70] Deliberation n°033–2010 of 11 February 2010 providing a first authorization of a simple biometric identification system (fingerprint) and deliberation n° 236–2012 of 12 July 2012 extending the experimentation with a multimodal biometric system (fingerprint and finger vein) in order to increase accuracy results.

[71] It is referred to as "*identitovigilenge*" in French.

[72] Deliberation n°33–2010, *op. cit.*

[73] Deliberation n°236–2012, *op. cit.*

[74] *Idem.*

[75] *Idem.*

[76] Deliberation n°324–2008 of 11 September 2008 authorizing the use of fingerprint stored in an individual device to control access to an Accommodation and Rehabilitation Centre.

[77] Deliberation n°492–2008 of 11 December 2008 refusing the installation of a biometric system relying on the storage of fingerprint in a badge to control access to a community home of young workers.

[78] Deliberation n°038–2008 of 7 February 2008 authorizing the support work centre (Centre d'Aide au Travail) « Le Vert Coteau » to install a biometric system to control the presence of mentally disabled at work.

[79] *Idem.*

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

the system relies on biometric data that do not leave a trace and that the individual's consent, in concertation with their family and legal representatives, will be respected. This decision constitutes an illustration where the requirement of decentralized storage is put aside considering the category of persons involved and the purpose of the system, which is more related to a "care" use of biometrics than a security-related use.

The potential expansion of such biometric uses raises, in our view, some important societal and legal questions. First, we observe that when taking into account possible alternative to biometrics, CNIL's analysis is much focused on technological solutions (badges with bar code and PIN code) and does not expressly address non-technological solutions, in particular a human accompanying framework. The biometric system and its characteristics (centralized storage and function of identification) are assessed on the basis of a "convenience" standard rather than a "necessity" standard. In our view, a much deeper reflection and concertation is needed on the "care" uses of biometrics in accompanying disabled individuals. Second, in these three decisions, the individuals enrolled in the system are vulnerable people, either due to social condition or disability, and much of the legitimacy of the system is derived from the individuals' consent to participate. This raises the question in our view of the extent to which vulnerable people may "freely" give consent to the processing of their biometric data and thus provide an adequate legal basis for such processing.

6.2. *Identification of candidates to an exam*

The CNIL authorized The Graduate Management Admission Council (GMAC) to deploy a biometric system based on palm vein recognition of candidate students to the Graduate Management Admission Test (GMAT), which is a worldwide exam organized to select candidates to MBA (Master of Business Administration) programmes.[80] The exam is indeed organized in identical conditions in about 110 countries each year for an average of 200,000 candidates, with the aim of selecting students for about 1800 MBA programmes and high schools worldwide. In France, 8 different centres are managed by the GMAC and about 2000 candidates take the GAMT exam each year. The goal of the biometric system is to avoid identity fraud, in particular the substitution of one candidate by another. GMAC reported past cases of proven fraud, notably in 2004 where 6 "professional candidates" took the exam in the place of 186 persons in exchange for remuneration.[81] Because of these cases of established fraud, GMAC justifies the deployment, in other countries, of an identification system of candidates based on their fingerprint in order to avoid identity substitution. In the case of France, and because of the restrictions imposed by the CNIL, GMAC proposed recourse to palm vein recognition, which is considered less intrusive as it is a biometric characteristic that is deemed without trace. The biometric systems nevertheless involve the centralized storage of the biometric templates in a central database in the United States of America, where the server is located. Retention of the biometric characteristics is planned for five years, which corresponds to the validity period of the exam.

This case is of particular interest in several respects. Firstly, it derogates to the CNIL's approach with respect to the legitimate basis of the biometric system. As we have seen, biometric systems pursuing a security-related objective generally invoke the protection of "legitimate interests" of the controller and are exempted from the necessity to obtain the individuals' consent. In contrast, biometric systems pursuing objectives linked to the fight against identity fraud, without any underlying "security" rationale, as is the case of the GMAT exam, have always been subject to prior individual consent (see *supra* "biometrics in school environment", "biometrics in commercial environment"). The GMAC decision therefore constitutes the first authorization of compulsory enrolment in a biometric system that does not pursue a security-related goal.

Secondly, this decision is remarkable as it authorizes a centralized storage of the biometric characteristics and an identification-matching process (1:n matching), which therefore involves important data protection risks. Again, in the absence of security-related justification, the CNIL generally requires the deployment of a system of verification (see *supra* for comparison "biometrics in the school environment"). This decision demonstrates that although the CNIL has elaborated a comprehensive proportionality policy (see *infra*), certain particular circumstances may lead the Supervisory Authority to revise and adapt the application of this policy. In this particular case, it is apparent that the worldwide character of the exam, with its high risk of fraud, on the one hand, and the criterion of capturing a biometric characteristic that does not leave trace on the other, were decisive in granting the authorization.[82] However, as we will see now, recent technological evolutions should lead the CNIL to deeply reconsider this approach.

7. Conditions of proportionality: evolution and perspectives

7.1. *CNIL's conditions of proportionality under evolution*

From 2005 to 2013, CNIL's methodology for the evaluation of biometric systems was said to be based on the following criteria: i) the distinction between "pressing security need" requiring the securitization of a delimited area representing a "*major stake, which surpasses the sole interest of the organization*" and more general securitization goals or identity management purposes; ii) the distinction between biometric data leaving a trace and biometric data leaving no trace; and iii) the place of storage of the biometric data, distinguishing the central storage in a server or in the reader and the storage

[80] Deliberation n°360–2009 of 18 June 2009 authorizing GMAC (Graduate Management Admission Council) represented by Pearson Education France to install a biometric system to control access to examination rooms in order to prevent identity fraud and substitution of candidates.

[81] CNIL's Annual activities report 2009, p. 55.

[82] See the interview of J.-F. Carrez, Commissioner at the CNIL in charge of "Education and superior education" in CNIL's Annual activities report 2009, p. 55, available here: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf (last accessed 1/11/2015).

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

in an individual device exclusively under the control of the data subject.

Another criterion, which is not formally expressed, relates to our view of the categories of persons enrolled in biometric systems and the legitimate basis associated with the processing of their biometric data. CNIL's approach indeed distinguishes two main categories of people/legitimate basis: i) the enrolment of employees in biometric systems relying on the legitimate interests of the organization (generally security-related purposes); ii) the enrolment of minors and customers (in general for identity management purposes) or volunteers (experimental and research purposes), the legitimate basis of which is the data subject's consent. The CNIL is indeed much stricter regarding the enrolment of minors and customers than employees for example. In turn, the CNIL is also stricter regarding the enrolment of minors than customers. The context of implementation of biometric systems (school, work *etc.*) is in practice, the primary criterion when assessing the proportionality of a system.

Technological developments have nevertheless led the CNIL to reconsider its policy, in particular, with respect to two of these criteria. First, the distinction between biometric data leaving a trace and biometric data leaving no trace is less and less relevant. Rapid technological evolutions show that biometric data that were not considered as "leaving trace" and thus susceptible to be captured and used without the knowledge of the individuals must now be considered as biometric data leaving a trace. A striking example is "face recognition". Multiple uses online make faces more and more subject to biometric identification. Another example is finger/hand vein recognition or iris recognition which tends to allow more and more contactless systems, thus paving the way to possible use without the knowledge of the individual. As noticed by E. Kindt, "*whether biometric characteristics can be captured with or without the presence and/or cooperation or knowledge of the data subject is not neutral as it depends on the state of the art of particular biometric technology at a given moment*",[83] implying that more biometric characteristics may leave traces over the years and become apt for hidden collection and comparison. Aware of these evolutions, the CNIL has abandoned this distinction since mid-2013. Along with E. Kindt, we believe this new approach is most welcome.

Second, concerned by the increasing recourse to biometric technologies to identify/authenticate individuals, the CNIL decided to launch in 2012 a deep reflection regarding the use of biometrics in an individual's everyday life.[84] The goal of the CNIL was to proactively address the multiplication of biometric identification in everyday life, from the work place to the use of biometric bank credit card or the identification of patients in hospitals, public services, commercial services etc. This led the CNIL to order a survey regarding the perception of biometrics by the French population. The results have showed that the French population widely admits the use of biometric identification by State authorities for national-security and/or forensic purposes.[85] While the use of biometric identification in the work environment receives mixed reactions, the French population is however clearly reluctant to accept the use of biometric technologies in a commercial context, including biometric contactless payment means or access control to catering or recreational spaces. As a whole, the French population showed itself reluctant to trivial uses of biometrics in everyday life.[86]

These elements are certainly at the basis of a shift in policy. The CNIL is considering emphasizing the categories of purposes pursued by the biometric system. Indeed, in the report on biometrics submitted to the Senate, the CNIL suggests a distinction between three types of systems:

1) *"Security-related biometric systems", which are those deemed indispensable. In those cases, the biometric system is exclusive and individuals cannot opt-out.*
2) *"Biometric systems as a service" (also called "biométrie de confort" or "convenience biometrics"). In these cases, the security claims are not sufficient to override individual's rights. As a consequence, individuals will have to be duly informed and explicitly consent to be enrolled. Alternative access control means shall be available in case of refusal.*
3) *"Biometric systems for research or experimental purposes".*[87]

Under such a renewed doctrine, the impact of the criterion relating to the category of people enrolled in a biometric system remains nevertheless unclear. Following this new approach, employees should consent to the processing of their biometric data when the system fails to satisfy the "strict-security" test under case 1. Indeed, we have seen that many biometric systems are not necessarily deployed in a context of "pressing security need", but can be deployed for more "general security purpose". Under the new approach of the CNIL, this second category of biometric systems should therefore fall under case n°2 and the individual's consent should become necessary. However, this renewed doctrine raises some difficulties in the work environment, where the validity of individual consent may be questioned. Indeed, according to the Working Party 29's opinion there is a strong presumption that employee's consent is invalid in the employment context, given the imbalance of power between the employee and the employer.[88] The Working Party 29 further asserted that the processing of biometric data in the context of employment would therefore preferably be based on another lawful ground.[89] Besides, certain biometric uses analysed in the present contribution may hardly fall into either of these categories, as for example the *GMAC* authorization (see *supra* "identification of candidates to

[83] Els Kindt, *op. cit.*, p. 655.

[84] CNIL Annual Activity Report 2012, p. 19, available here: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_RA2012_web.pdf (last accessed 1/11/2015).

[85] Sandra HOIBIAN, « Les Français se montrent réservés sur l'usage de la biométrie dans la vie quotidienne », Report of the CREDOC (Centre de Recherches pour l'Etude et l'Observation des Conditions de Vie), May 2013, available here: http://www.credoc.fr/publications/abstract.php?ref=R291 (last accessed 1/11/2015).

[86] *Idem*.

[87] Report of Senator François Pillet to the Senate of 16 April 2014, *op. cit.*, pp. 13–14.

[88] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011, WP187.

[89] Article 29 Data Protection Working Party, *Opinion 03/2012 on developments in biometric technologies*, 27 April 2012, WP193, p. 11.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013

an exam"). As a consequence, the CNIL's new approach would restrict the use of biometric systems and possibly prevent new biometric uses from emerging.

7.2. *Towards a condition of "strict security need"?*

In May 2014, the French Senate adopted a bill of law destined to limit the use of biometric technologies.[90] The goal of the proposal is to frame CNIL's power of authorizations for biometric systems in the private sector in compliance with article 25.I 8° of the Data Protection Act.[91] Under this proposal, the processing of biometric data shall be limited to cases of "*strict security necessity*", understood as "*the protection of physical integrity of persons, the protection of goods or information the disclosure or destruction of which would cause serious and irreversible harm and which responds to a need that surpasses the strict interest of the organization*." The formulation appears in part inspired by CNIL's policy with respect to the storage of fingerprints in central databases. The consequences of such a proposal, if adopted by the Legislator, would be quite significant for the biometric industry.

Under the proposed framework, all uses that fail to satisfy this "strict security need" criterion would be forbidden. This implies that all current uses of biometrics that rely on individuals' consent, such as the use of biometrics in schools and for the provision/access to commercial services, would simply become illegal, closing the door to any biometric developments in the private sector outside security-related motivations. Although it is most welcomed that the Legislator endorses the responsibility to frame the use of biometrics in the private sector, we believe that Senator Gorse's proposition is not necessarily adequate, as it states once for all which biometric use is admissible or not and does not leave sufficient margin of appreciation, considering possible beneficial use of biometrics in society outside the field of "security". Although technical and security aspects are not central to the present paper, we believe such a legislative approach disregards potential technological security developments applied to biometrics: in the field of encryption, revocability, irreversibility and the unpopularity of templates, which are promising with regard to limiting the data protection risks generated by the processing of biometric data.[92]

8. Conclusions

CNIL's experience in applying a proportionality test to biometric systems installed in the private sector is of interest as it contributes to illustrate, in concrete situations, where biometric systems are currently expanding. In general, the CNIL has proven to be quite consistent in applying its proportionality policy over the last decade.

The CNIL long relied on the type of biometric data (with trace and without trace) and type of storage (centralised and decentralized) to assess the impacts of a given system on individuals' rights. We believe that since the distinction between biometric data leaving a trace and biometric data leaving no trace is no longer relevant, the CNIL should instead put more emphasis on the type of system (verification or identification) and the place of storage when carrying out the assessment.[93]

Besides design characteristics, the category of people enrolled and the context in which the biometric system is to be deployed, constitute crucial criteria in CNIL's evaluation. In practice, the CNIL applies two standards of review, which are essentially related to the legitimate basis of the processing. In cases where the legitimacy of the biometric system will rely on legitimate interests of the data controller, the necessity test will be applied quite strictly. In contrast, where an individual's consent is required, the necessity test will be applied more loosely. As a result, individual consent becomes the condition for the installation of a biometric system outside security-related motivations. Respect for freely given, informed and specific consent is critical but crucial, and requires a strict interpretation.

The recent legislative proposal intended to limit the use of biometrics to strict security situations may also limit the development of biometrics outside the traditional borders of security. We believe that such a proposal has the merit of generating a necessary debate with regard to the expansion of biometrics in the everyday life. However, we also believe that the Legislator should not be too prescriptive, in order to leave space4 for technical innovations and potential beneficial uses of biometrics in new areas where identity management is crucial.

Acknowledgment

This paper was made possible thanks to the funding from the PARIS project (PrivAcy PReserving Infrastructure for Surveillance), sponsored by the European Union Seventh Framework Programme, under Grant Agreement No: 312504. However, the paper is merely representing the author's view and is not binding PARIS partners or the European Commission.

[90] Legislative proposal limiting the use of biometric technologies adopted by the Senate on 27 May 2014, available here http://www.assemblee-nationale.fr/14/propositions/pion1972.asp (last accessed 1/11/2015).

[91] See the Report of Senator François Pillet to the Senate, *op. cit.*

[92] Patrizio Campisi (ed.), *Security and Privacy in Biometrics*, Springer, 2013.

[93] See also Els Kindt, *op. cit.*, pp. 647–654.

Please cite this article in press as: Claire Gayrel, The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.013