Pierre Piazza

DO POLICEMEN DREAM OF BIOMETRIC CHIPS? HOW NEW TECHNOLOGIES ARE CHANGING LAW ENFORCEMENT IN WESTERN COUNTRIES

It was in France, at the Paris *préfecture de Police*, during the last three decades of the nineteenth century, that the process of rationalizing police identification techniques reached a high point: with the advent of *Bertillonnage*, an identification system that focused mainly on measuring certain portions of the human skeleton, the body of individuals became an object of knowledge *per se*.[1] The trend continued with the onset of the twentieth century, when complex knowledge of fingerprints and their classification emerged, ultimately prompting many police forces across the globe to create their own huge dactylo-scopic file systems.[2]

Today, as legitimate heir to these early policing attempts, biometric technology is viewed as incontrovertible among public policymakers in charge of security issues. "Biometric technology" refers to a variety of processes, all of which aim at establishing with quasi-absolute certainty who is who, by turning utterly personal characteristics—be they physical, physiological, or behavioural—into a digital footprint. Over the last few years, this technology has triggered the development of especially two types of devices in the field of security: biometric

databases have been built, and biometric data-laden microchips have been embedded into ID or travel documents.

In France, the automated fingerprint database (*Fichier automatisé des empreintes digitales or FAED*) was launched in 1987 and became the first computerized biometric file system to operate on a national scale in 1994. Stored and preserved in it are the fingerprints of all individuals prosecuted for serious offences. Personal records of nearly 3 million people are currently stored there. In addition, an automated national database of genetic data (*Fichier national automatisé des empreintes génétiques or FNAEG*) was created in 1998. Although initially targeted specifically at sexual offenders, this database has become "a 'general-purpose' criminal identification tool,"[3] following in particular the bill on interior security passed on March 18, 2003.

However, criminal identification needs do not fully account for the actual use of biometrics by the French authorities. An increasingly routine application is foreigner identification. As early as 1997, the Debré law already provided for taking the fingerprints of foreigners either applying for a residence permit, arrested on the French territory as illegal residents, or subjected to a removal order. The bill was then supplemented by a statutory provision of the immigration control act of November 26, 2003, which established the taking and automated processing of visa applicants' fingerprints. From 2005 onwards, France—as part of the *BIOmetric Data Experimented in Visas* project—experimented with this process in several of its consulates throughout North and Sub-Saharan Africa, Asia, and Europe.[4] The experiments revolved around the Visa Information System project that the European Council, by a decision of

June 8, 2004, decided to implement in 2008. Based on the *Schengen Information System II* technical framework, this database is destined to become one of the largest centralized biometric repositories in the world, storing the fingerprints of almost 70 million individuals deemed liable to penetrate or transit through the Schengen area.[5] At the European level, this tool will supplement the EURODAC database, which has been in operation since January 2003 and is used to collect and match the fingerprints of illegal migrants as well as all asylum seekers aged fourteen or older.[6] It should be added that we are currently witnessing an expansion of the field of application of the various biometric file systems operated in Europe, gradually integrated into a single network, as evidenced by the Treaty of Prüm, signed in May 2005. This treaty, which provides for the circulation of dactyloscopic data and DNA profiles among seven EU member States, was fully incorporated in the legislative framework of the EU as of June 2008.

Ever since the 9/11 attacks, biometric technologies have continuously found new application areas, owing to US pressure on the European Union. The implementation by US authorities, in the context of the "war on terror," of biometric control programs targeting incoming foreigners (in particular the US-VISIT program) prompted European countries to deliver biometric passports to their own nationals. Such documents had become necessary for two reasons: first, in order to skip the visa procedure when travelling to the USA; second, to comply with the new clearance formalities enacted at US borders, which required digital readout of biometric data embedded in travel documents and the possibility for security services to match this data with information extracted from other data-

bases. This explains why the European Commission, with its December 13, 2004 regulation—and in compliance with the recommendations of the International Civil Aviation Organisation (ICAO)— "biometrized" the passports of all citizens of the European Union.

Finally, over the last few years, many countries also felt the need to implement biometric IDs for their nationals.[7] Thus, the INES project was hinted at by the French Minister of Interior in 2003, before spurring a nation-wide debate two years later. This project, which involved embedding the new ID with distinctive individual biometric data encapsulated in a remotely readable chip, was eventually shelved by Nicolas Sarkozy in June 2005, mostly because of the strong outcry it had raised.

Thus the recent past has seen a considerable rise of biometrics—established, in the name of the struggle against risks, threats, and dangers deriving mainly from the ever-increasing circulation of individuals around the globe, as the ultimate and vital high-tech answer to our security issues. This extension of biometric schemes to large bodies of populations raises some issues regarding not only the policing rationales underlying these dynamics, but also their repercussions on individuals, who are being subjected to hitherto unknown constraints.

THE MYTH OF INFALLIBILITY

More often than not, in an attempt to justify the imperious necessity of biometrics, police authorities will present them as a "miracle solution" that will reveal the true identity of individuals. The technology, however, is far from absolutely reliable.[8] In 2003, P. Wolf (Training Centre Manager at the

Central office for Information Systems Security, attached to the General Secretariat of French National Defence), had publicly debunked the mythical almightiness of certain biometric devices by pointing out some of their flaws, as well as the lack of any rigorous and independent process of performance evaluation.[9] One year later, the European Data Protection Authorities group also voiced serious concern regarding the introduction of biometric elements into passports, on the grounds that their efficiency was still unproved and that they tended to cause many mistakes. More recently, in France, the National Ethics Advisory Committee again highlighted the weakness of the transmission process of biometric data loaded in passport chips, with major consequences in terms of "confidentiality." In 2007, researchers in cryptography from Leuven University, using a basic RFID reader available at the store next door, managed to read confidential data stored in several Belgian e-passports.

There is no such thing as a zero-error rate as far as biometric databases are concerned, either during the recording process or in terms of "false positives" in the subsequent control phase—in fact, theses rates vary according to the type of biometric identifier considered. While, according to B. Didier, scientific and business development director in the security division of Sagem Défense Sécurité, these error rates have been brought down to 1–2 percent in the case of iris recognition (iris being the most reliable identifier, along with fingerprints),[10] their impact is anything but trivial when identity checks are performed against very large databases: in the case of a 60-million-entry database, such an error margin might affect 60,000–120,000 individuals. The first official audit report on Eurodac

(published in July 2007) actually mentions much larger error rates: fully 6 percent of the fingerprints stored in this European biometric database had to be discarded owing to their poor quality.

FUZZY PATTERNS OF JUSTIFICATION

The case made by law enforcement authorities for the absolute necessity of using biometrics for security purposes is a much debatable one, as evidenced by the emblematic story of INES, when biometrizing the national ID card was put forward as a crucial need by the French Interior Ministry, with the aim of improving the fight against document forgery. The Ministry, however, was unable to precisely quantify the magnitude of this fraud in the country.

Moreover, the Interior Ministry, adamant that establishing a biometric ID card had become an inescapable step in the fight against terrorism,[11] failed to fully demonstrate just how such a document might contribute to the cause. Many key questions were left unanswered: How important is the role assigned to the national ID card in the *modus operandi* of terrorists? How could a biometric national ID card help identify would-be terrorists? What kind of benefit could the police expect from a biometric national ID card when confronting terrorists who, being nationals themselves, could legally obtain this document?[12]

Finally, while the Ministry of Interior tried to legitimize the INES project by arguing that it had the unavoidable duty to comply with supranational measures, neither the norms promulgated by ICAO nor the European Regulation of December 13, 2004 specifically mentioned national ID cards. As M.

Marzouki explains, "presenting as an unsolicited duty the implementation of international or regional political decisions in which France was fully involved, and sometimes even instrumental, constitutes what some NGOs have called 'political laundering.'"[13]

A SIGNIFICANT STRENGTHENING OF POLICE POWERS

Biometrics enable law enforcement authorities to significantly increase their prerogatives by building population databases, a process that goes virtually unchecked, even though one would expect widespread democratic debate in such a case. Such a database was, for example, implemented in Australia, and originally listed mostly paupers, misfits, and aborigines in order to control them more closely.[14] In France, the Ministry of Interior, disregarding strong reservations by the CNIL,[15] simply decreed on April 30, 2008 that a central database was to record the digital pictures of all owners of biometric passports, as well as eight of their fingerprints.[16]

Furthermore, one cannot help but notice a sharp rise in the flow of biometric data pouring from ever-larger national and supranational databases (this is made possible by the frequent use of certain biometric identifiers which tend to become almost universal). In addition to this, a new—quite symptomatic—trend is illustrated by the implementation of the US-VISIT program[17] in the USA: not only is biometric data about individuals, once gathered and stored, cross-referenced with various public databases containing information relative to the status or habits of the person in question, it is also checked against suspect lists.

An expansion and strengthening of policing powers is thus taking shape via the amplification of ever more globalised, intrusive surveillance practices, which are no longer strictly justified by authentication and identification goals. Those surveillance practices rely nowadays on large-scale schemes based on the accumulation, exchange, and exploitation of countless biometric elements used to track down individuals, who can now be remotely identified, located, and followed, their movements strictly monitored in both time and space.

In addition, these surveillance practices help establish a social sorting of individuals. The sorting criteria organize threat levels into a hierarchy and are used to establish "risk profiles" that tend to discriminate against some individuals according to features pertaining to their religious practices, nationality, and/ or ethnic origin.[18] For instance, travellers entering the United States will automatically be labelled by local security authorities, either as "trustworthy," "questionable," or "dangerous."[19]

The EU is fully involved in this dual process, with initiatives that encourage law enforcement authorities to build and use a host of biometric databases intended to be made "interoperable": "profiling" of individuals on the one hand, and increased tracking of their movements on the other—a radical change in the approach of security issues. As highlighted by V. Mitsilegas, the monitoring processes of terrorism, crime, and immigration have been tightly interwoven—especially since 9/11—into the fabric of a "securitarian continuum," which highlights the advent of a "world vision" that "raises fundamental issues about the criminalizing of immigrants and the naming of the 'other.'"[20]

The extension of this surveillance logic to ever larger and diverse bodies of the population, including foreigners as well as nationals, certainly plays a pivotal role in sketching the figure of a new enemy from questionable criteria of suspicion and "undesirability." Not only does this trend contribute to breeding incomprehension, humiliation, and resentment among those being stigmatized,[21] it also raises major issues in terms of protection of fundamental rights.

INSUFFICIENT PROTECTION FOR INDIVIDUALS

The use of biometric data by police forces raises key privacy and liberty issues. Precisely which authorities are using the collected data? How do they actually use and mobilize it so as to reach only the officially stated goals? As rightly pointed out by lawyer A. Weber, this issue is of particular consequence whenever a given State seizes and exploits biometric data pertaining to other nationals: "Anybody who travels to the United States with a biometric passport is entrusting their data to perfect strangers, with no knowledge of who is going to process this data, how it is going to circulate, how and how long it will be stored in the databases. The French State is taking the matter rather lightly as far as its nationals are concerned, even though ensuring the safety of their personal data is one of its most imperious obligations. We are left with a massive black hole, and no clue whatsoever . . . ."[22]

Is biometric data collected with the consent of individuals or unbeknownst to them? As some industrial players readily admit, new technologies allow "on the fly" capture of biometric data (facial features, irises) and several experiments in biometric CCTV surveillance—in Newham and Birmingham, UK,

for instance—have shown that anonymity of the public space is seriously at risk.[23]

Are the agencies in charge of controlling biometric databases endowed with sufficient investigative and enforcement power to efficiently protect individuals, as is their mission? Half the member countries of ICAO do not even feature such agencies.[24] Moreover, when they do exist, their role is often quite restricted. Such is the case of the CNIL in France. The agency is expected to act despite the lack of any proper legal framework for biometrics; the creation of security databases is only subjected to mere advisory pronouncements by the CNIL; its budget and human resources prove insufficient; finally, its framework for action remains the Act of 6 January 1978, somewhat inadequate perhaps in this era of international circulation of biometric data.[25]

Similarly, the protection of individuals at the European level is becoming an extremely formal affair, given the current profusion of legal texts, often conflicting and hardly legible,[26] as well as the inefficiency of the European Data Protection Working Party (yet another advisory board whose rulings are simply not binding for EU decision makers), not to mention the weak sanctioning power of the European Data Protection Supervisor. This is compounded by the inadequacy of awareness campaigns led on this crucial issue, despite the many expectations citizens have in this area, as highlighted by a recent Eurobarometer survey on data protection within the EU (February 2008). Meanwhile, in the USA, privately-held companies, such as US Search, busily engage in trading personal data, and the concept of "privacy," though allegedly protected

by the Fourth Amendment to the Constitution, is not being considered a fundamental right at all.

THE DANGERS OF A RIGID CONCEPTION OF IDENTITY

The development of biometrics-based policing is undermining the idea of individual identity at its very core. Physiological characteristics are increasingly being favoured as authoritative sources of information about individuals. When mobilizing them in the name of security imperatives, police forces make our bodies do all the talking, defining who individuals are without ever bothering about their social and cultural background. Their identity will be revealed and fixed regardless of what they might think, say, or believe; it will be reduced to some kind of stable, permanent, and unambiguous "electronic double" which, however disconnected from the actual persons, is henceforth viewed as an "absolute truth," at any rate more so than their actual flesh and blood.[27] Hence, a dematerialized conception of identity, based exclusively on objectivised criteria captured from the body itself, tends to replace a more subtle model that takes into account the complexity of a constantly evolving individual identity.

This process of reification, which leads individuals to lose their own singularity as their living experience is being reduced to mere biometric parameters, is fraught with danger: individuals are locked up within a permanent, encoded, and immutable bodily identity, and denied any opportunity for negotiation through social exchanges. Specifically, what these new forms of identity assignment actually challenge is the social importance of trust and the mediation of communication and language: "A

whole series of narratives are giving us to understand that the individual's intervention is laden with fraud and falsehood. This type of bureaucratic suspicion lurking behind scientific certainty must be thwarted."[28]

The inherent logic of biometric technologies also allows them to function in an almost autarkic fashion and gradually conquer their autonomy from society by acting exclusively within the framework of a digital representation of reality. Thus, a technical law, utterly disconnected from the specific backgrounds, values, and feelings of the individuals who constitute the social world in practice, is becoming the norm.

This phenomenon incidentally has a major impact on the practices of security agencies, so much so that it paradoxically tends to deeply alter the very mechanisms that were meant to safeguard their efficiency. This is highlighted by G. Dubey, drawing on his research about the use of biometric technologies by French border police officers: "Within the PAF (*Police de l'Air et des Frontières* or Air and Borders Police), the most senior officers, endowed with both experience and informal know-how, often express concern at the evolutions affecting statutory and documentary controls. . . . Identification seems to gradually lean towards self-sustainability. The process of matching biometric—i.e. formal—identity against information stored in the database is taking precedence over that of conducting interviews and checking reception conditions. . . . The automated processing of identification, reliable as it is supposed to be, 'captures the attention' to such an extent that the PAF is ultimately diverted from the core tasks of its mission."[29]

NOTES

1   P. Piazza, *Histoire de la carte nationale d'identité*, Odile Jacob, Paris, 2004.

2   On early attempts, by the US government, at fingerprint-based identification of thousands of Chinese migrants in California, see S. A. Cole, *Suspect identities*, Cambridge, Harvard University Press, 2001.

3   Work group on police and gendarmerie files, *Fichier de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion*, La Documentation française, Paris, 2006.

4   S. Crépeau, G. Dubey et X. Guchet, *Biodev : la biométrie dans les visas. Du contrôle à distance au macro-système technique*, final report INT/ministère de l'Intérieur/Civipol, 2006

5   *See* Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008

6   D. Broeders, "The New Digital Borders of Europe : UE Databases and the Surveillance of Irregular Migrants," *International Sociology*, vol. 22, n° 1, 2007.

7   C. J. Bennett et D. Lyon (eds.), *Playing the Identity Card. Surveillance, Security and Identification in Global Perpective*, New York, Routledge, 2008.

8   On the "fetichized" view of biometric facial recognition technologies in the US in the wake of 9/11, in spite of a questionable record of efficiency, see K. A. Gates, "Wanted Dead or Digitized. Facial Recognition Technology and Privacy," *Television & New Media*, 2002, n° 3.

9   P. Wolf, "De l'authentification biométrique," *Infosécu*, n° 46, October 2003.

10 B. Didier, 4 May 2006, Hearing on biometrics by the French parliamentary office of scientific and technological choices. Report n° 3302, Assemblée Nationale, 8 September 2006.

11 On the recurrence of this claim by public authorities in order to justify the use of biometric technologies, see A. Garapon et M. Foessel, "Biométrie, les nouvelles formes de l'identité," *Esprit*, Aug.-Sept. 2006.

12 L. Laniel et P. Piazza, "L'encartement comme réponse au terrorisme (France/Grande-Bretagne)?" in X. Crettiez and P. Piazza (eds.), *Du papier à la biométrie. Identifier les individus,* Presses de science po, Paris, 2006.

13 M. Marzouki, "La loi informatique et libertés de 1978 à 2004 : du scandale pour les libertés à une culture de la sécurité" in I*nformatique : servitude ou libertés*?, Sénat éditions, Paris, 2007.

14 D. Wilson, "Australian Biometrics and Global Surveillance, *International Criminal Justice Review*, vol. 17, n° 3, 2007.

15 Created by the law of 6 January, 1978, the CNIL (National Commission for Information Technology and Liberties) is an independent administrative authority protecting privacy and personal data.

16 P. Piazza, "La mise en œuvre du passeport biométrique en France : quelques réflexions sur les modes d'action du ministère de l'Intérieur, Blogclaris, 31 mai 2008 : http://groupeclaris.wordpress.com/?s=piazza

17 L. Amoore, "Biometric borders. Governing mobilities in the war on terror," *Political Geography*, vol. 25, n° 3, 2006.

18 D. Lyon, "Surveillance, Security and Social Sorting," *International Criminal Justice Review*, vol. 17, n° 3, 2007.

19 N. Morgan et A. Pritchard, "Security and social 'sorting': traversing the surveillance-tourism dialectic," *Tourist Studies*, vol. 5, n° 2, 2005.

20 V. Mitsilegas, "Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme," *Cultures et conflits,* n° 58, Feb. 2005.

21 Afghan asylum seekers went as far as burning off their fingertips to signify their refusal to be filed in the EURODAC biometric database, see D. Bigo, "Le visa Schengen et le recours à la biométrie" in X. Crettiez and P. Piazza (eds.), *Du papier à la biométrie*, op. cit.

22 A. Weber, 4 May 2006, Hearings on biometrics by the parliamentary office …, *op. cit.*

23 D. Murakami Wood (ed.), "A Report on the Surveillance Society - For the Information Commissioner by the Surveillance Studies Network," September 2006 : http://www.libertysecurity.org/IMG/pdf_Surveillance_society_full_report_final.pdf

24 A. Ceyhan, "Enjeux d'identification et de surveillance à l'heure de la biométrie," *Cultures et conflits*, n° 64, Winter 2006.

25 C. Lacouette-Fougère, *La CNIL face à la biométrie : heurs et malheurs d'un régulateur*, Thesis, Toulouse IEP, 2007.

26 S. Preuss-Laussinotte, "Bases de données personnelles et politiques de sécurité : une protection illusoire?", *Cultures et conflits*, n° 64, Winter 2006.

27 I. van der Ploeg, "Written on the body: Biometrics and identity," *Computer and Society*, vol. 29, n° 1, 1999 ; K. F. Aas, "'The body does not lie': Identity, risk and trust in technoculture," *Crime, Media, Culture*, vol. 2, n° 2, 2006.

28 D. Bigo, CNIL hearing on the INES project, 2005.

29 G. Dubey, "Le grand décrochage. Le cas des systèmes d'identification biométriques," communication presented at the 14th CREIS colloquium "Informatique et société," Paris, 14-15 June 2007.