Biometrics and new forms of identity

Michaël Fœssel and Antoine Garapon

Biometrics is the science and technology of identification and authentification which consists of transforming biological, morphological or behavioural characteristics into a digital fingerprint. Its purpose is to confirm the uniqueness of a person by measuring a part of their body that cannot be changed or controlled.[1]

Biometric identification is one of the most promising instruments for today's battle against terrorists, particularly in the United States of America which has imposed it on a number of its partners, including Europe. That is why Great Britain has decided to introduce a biometric identity card, while in France, a similar plan to introduce a medical identity card, the "Carte Vitale" has reached an advanced stage. Apart from the internal benefits (notably the reduction of fraud with the "Carte Vitale"), the expected benefits include improved immigration and border controls. This supposedly inviolable form of control creates the feeling of being able to manage a security "black hole" so to speak, where illegal immigration converges with trafficking and terrorism. This explains the success of biometric identification technology and the hopes vested in it by governments and the governed alike. How else can the relative passivity of public opinion in the face of an increasingly widespread phenomenon be explained? When the uses of biometrics are challenged, it is on the basis of their general effects and not in relation to the fight against terrorism.[2] To explain this relative public apathy, we put forward the theory that the justification for biometrics is rooted in the nature of contemporary terrorism: from one phenomenon to the other, a whole rationale for security action is being put into place.

Terrorist threat and biometric response

The widespread use of biometrics and the forms of identification it permits can be justified first of all by the anonymity that is the hallmark of terrorist action (and actors). "To identify" always means to make the unknown known, by means of relatively stable recognition criteria. It has to be admitted that globalised terrorism does not offer such criteria and it is therefore legitimate to seek to reconstitute them afresh. In a recent decision (the conclusions of which were confirmed by the London bombings of July 2005), the House of Lords noted that British subjects could prove just as much a threat to national security as foreign nationals.[3] This fluidity implies that the boundary dividing "terrorists" from the rest of the population is less commonly defined on the basis of nationality. Divisions now prevail that cut across nations themselves. In a context where the suspect is not necessarily a foreigner, a new arrival or even an activist, the figure of the "enemy within" emerges, an enemy who appears to elude all the classic identification procedures.

Biometrics seems to offer an appropriate and efficient response to this erosion of the traditional dangerousness criteria. Biometric parameters effectively identify an individual

without taking account of his or her nationality or community affiliation, using criteria that do not draw on a person's life history in any way.[4] And because it identifies individuals in this way, biometrics makes it possible to track them. The most pertinent comparison is probably that of tracking goods being transported in compliance with the principle of traceability: in both cases it is a question of identifying individuals, storing details of their itineraries and deducing a level of threat from the nature of the movements observed. The characteristic of the individual (thing or person) is of little consequence, let alone their political, ethnic or religious identity. The only useful criteria are those that are entirely objective and can be used to locate the individual.

Biometrics therefore fits into a context where "surveillance is becoming increasingly deterritorialised and intrusive".[5] But if modern-day terrorism justifies this development in surveillance technologies, it is because it is itself deterritorialised and intrusive, so terrorism and biometric recognition go hand in hand. Given this mutual implication, it is a matter of facing up to new uncertainties that seem to call for a technological response almost automatically. Terrorism effectively denotes a strategy of non-discrimination which expresses itself in different ways: a blurring of the distinctions between civilians and fighters, between "victims" and "culprits" and between public and private. This last aspect is decisive for the problem that concerns us: phenomenologically, the terrorist attack embodies the removal of the distinction between front and rear in favour of indistinct places (private and public) like the street, the metro entrance or the airport. The terrorist strategy is thus a strategy of ubiquity: it is a matter of convincing the "enemy" that any space can, at any time, become a battleground.

But there is one condition that is necessary for the implementation of this strategy: the anonymity of the terrorist. As Dominique Linhardt points out, the terrorist "melts into the obscurity of the common people" taking on the guise of the peaceful civilian down to the tiniest detail.[6] It can even be said that the terrorist overturns the democratic principle of presumed innocence: he needs to look like "someone who is harmless" to imbue his act with the maximum significance. The terrorist attack therefore constitutes a radical subversion of the norm having begun by apparently respecting it; in every case it is a question of causing terror from a neutral place (the common space) and in a seemingly comforting setting (the day-to-day) by suddenly making the most common objects behave unpredictably (the car explodes when the ignition is switched on, the metro is derailed, water is poisoned). This strategy is necessary both to make the occurrence of the act appear random, and its effects incalculable.

Consequently, terrorism relies on a strategy of delayed visibility. Anonymity and indistinctness must be succeeded suddenly and violently by a form of massive publicity, transmitted by the media. It is at this articulation point, between concealment and visibility, that biometrics is situated. Biometrics makes it possible to establish identification criteria that are stable since they are computerised and encoded in a universal language, and permanent since they are rooted in the permanence of the body. The presupposition of such a procedure is that the body is the only thing that a person is unable to lose at a time when no

other identifier (cultural, political or even biographical) is impervious to the indistinctness that is specific to terrorist action. It is therefore the body's inertia that is needed to thwart cover-up strategies.

But which body do we mean? In no case the real body which provides no reliable basis for recognition, or even the physical body which is also subject to the vagaries of time and the possibility of disguise. The body that interests biometric technology is a paradoxical body since it is both objectivised (reducible to computer parameters) and natural (inalterable). It is even, strictly speaking, a metonymic body as is attested by the importance of the iris as a particularly important organ of biometric recognition: this organ, whose biological parameters are unalterable, denotes a principle of constancy.

A redefinition of borders

The emergence of globalised terrorism is in no way responsible for the increased use of biometrics in security procedures. Rather than marking an abrupt change, the events of September 11 "revealed and accelerated a security process that had been ongoing since the end of bipolarity".[7] And so, while the first experiments go back to the 1950s, biometrics became widespread from the time when clashes linked to the Cold War gave way to transnational violence and infringements. Apart from espionage cases, bipolarity effectively drew a clear demarcation line between friends and foes, and the "dangerousness" of an individual could be inferred from his ideological marking.

There is, however, a very strong link between the depoliticisation of conflicts and the increased technicalisation of security procedures: biometrics is the result of a new understanding of borders and is helping redefine them. The first biometric policies go back to the "war on drugs" decreed by the United States government in the 1980s. This "war", which heralded in many ways the 21st-century "war on terrorism", is a conflict of a transnational type: the problem is that of fighting against anarchic movements of goods and persons and not against localised, homogenous groups. In this context, the figure of the drug trafficker is similar to that of the illegal immigrant: in both cases, police activity takes place at the border (the United States-Mexico border to be specific). So it is understandable why the border has become a favourite terrain for the experimentation of biometric techniques, with the involvement of no fewer than 54 security agencies to control entries into Texas and California.

In the United States, the full import of these new surveillance and control techniques can be appreciated if they are put in the context of *Homeland Security*, a concept based on the presupposition (heightened since September 11) that the national territory is vulnerable. Set up in 2003, the Department of Homeland Security represents the institutional unification of several security agencies around a single objective: "The prevention, deterrence, and preemption of, and defense against, aggression targeted at U.S. territory, sovereignty, population, and infrastructure."[8]

Far from strengthening the role of the border as a spatial limit, the use of biometrics contributes to the "dematerialisation" and the "deformalisation" of the border. It cannot be a question of a pure and simple turning inwards or a return to autarchy that would signify a break vis-à-vis the most basic demands of international trade. As such, America's decisions after September 11 concerning the border with Canada (and then, later, trade with Europe) are highly revealing. To secure their northern border while avoiding putting their own country in an embargo situation, in December 2001, the USA put in place a series of agreements entitled *Smart Borders*. This system, agreed with Canada, brings biometric recognition measures into general use, forming the basis of a differentiation between the

"good foreigner" (tourist or business traveller) and the "bad" (terrorist or trafficker).

Biometrics makes possible what traditional border control mechanisms made impossible, and that is risk anticipation prior to arrival at the border. By feeding biometric data (fingerprints, iris, voice, etc.) into computerised databases, the state is able to detect groups of undesirable individuals before they materially reach the border. This also applies to France which uses biometrics in numerous consulates in Africa, and computerised checking in embassies, airports and private companies, as well as airline companies. Here, we are

witnessing a change in surveillance methods, which no longer operate directly, but remotely.

Of course, biometrics is not the source of this remote surveillance paradigm. As Didier Bigo has shown,[9] the security agencies (both public and private) have long been involved in "security fields" rather than confined, stable areas. Security branches of the police, in particular, differ from criminal investigation branches by the indeterminate and immaterial nature of their field of action: for them, it has always been a matter of "remote surveillance" in other words, the process that consists of inferring the dangerousness of an individual from his or her movements. But, with biometrics, surveillance is built entirely on *a priori* principles, which implies the constitution of a system for classifying movements according

to their presumed significance.

With biometric control, the border loses its status as a geographical demarcation to become both functional and virtual. It is "deformalised" in the sense that it no longer designates a dividing line between two spaces and two sovereignties, but a control zone that must permit the distinction between dangerous individuals and others. This "zone" itself tends to become virtual, constructed exclusively on the basis of computerised parameters. From the moment a foreigner applies for a visa at the consulate he or she is identified using biometric characterisations that are stored in database. This completely new form of remote identification results in the transformation of the border from a line to an "act": it is the state that defines a frontier – that is ideally impassable – between an individual and its territory, and this frontier begins in an arbitrary manner, in the place where the individual in question

happens to be.

Rather than a globalisation of surveillance methods, we are witnessing the spread of controls beyond the traditional territorial confines of the exercise of sovereignty. Contrary to its

classical definition, the border loses its spatial nature: it must be everywhere and nowhere, as is illustrated by the deterritorialisation of controls.[10] Biometrics produces information whereby each individual becomes their own territory, so to speak, instigating a completely new kind of geography of the human body. The border is no longer a physical, geographical reality: it is the affirmation of power. It begins with the capability of scientifically establishing each person's uniqueness and then goes on to distinguish infallibly between people from the same territory. It no longer follows geographical contours but cuts through

people.

The depoliticisation of identities

The spread of biometric recognition technology has given rise to numerous interpretations of the nature of power in technologised democracies. Among these, the dominant theory is unquestionably that which links biometrics to the biopolitical paradigm and makes the computerised and security processing of the body the most spectacular sign of the insinuation of technologised power into private lives. Giorgio Agamben likens the biometric system for tracking individuals to "bio-political tattooing", a marking procedure that provides a continuum between the world of the concentration camp and contemporary democracies.[11] Biometrics "concerns the enrolment and the filing away of the most private and incommunicable aspect of subjectivity"[12] and brings to its conclusion a process of the body being captured by the authorities. Furthermore, this attack on the private (identified here as the body) which should be an exception, is tending to become the norm,

illustrating Agamben's famous theory that the state of exception is the true source of law.

This criticism is right to condemn the identification of the political with the limited sphere of the biological. But the equivalence between subjectivity and the individual biological body which is presupposed here is questionable. It is particularly debatable to claim to grasp the (biopolitical) essence of power on the basis of one of its most spectacular contemporary manifestations. The claim that biometrics is at the root of power is not only excessive, it also risks being blinding since the main effect of this procedure on the methods of recognition

and surveillance remains unknown.

Biometrics effectively propounds a specific concept of individual and personal identity, and it is this concept, if it were to become exclusive of all the others, that should be criticised. First it must be noted that biometrics produces a form of depoliticisation and of individualisation of surveillance that is different from the "panoptic" form advocated by Michel Foucault. For the state, it is no longer a matter of seeing all without being seen, but rather of interfering in the most extreme aspects of individual existence and reducing it to a sum of constant, objectivised parameters. It is therefore not necessary to "see all", but rather, to echo other Foucauldian terms, to "see as little as possible" preferring "a visibility freed from all other sensory burdens"[13]. Biometrics, like any classifying science, only deals with "screened objects", in other words figures and movements. It is interested not in the substance of beings but in constituting a "taxonomic area of visibility" which makes it possible to separate out individuals according to their dangerousness. Through this form of

abstraction that is characteristic of biometrics, we are reminded that there is power only over signs and not over bodies.

But the chief effect of this reduction of the body to computerised parameters is to privilege exclusively what Paul Ricœur called "idem-identity" (sameness) at the expense of "ipse-identity" (selfhood)."[14] To recognise this form of identity, "one compares the individual present to material marks held to be the irrecusable traces of his earlier presence in the very places at issue."[15] The biometric identity is reconstituted from a system of marks inscribed on the individual's objectivised body. From this point of view, biometrics identifies the body with a "relational invariant" which shields the doings of one individual in a given time from the slightest doubt. The criterion of similarity becomes perfectly constant since it is referred to the body's invariant structures. Biometrics could therefore be said to attain an "uninterrupted continuity", a principle that has eluded the branch of philosophy concerned with the ontology of substance.

The risk is that of a totalisation of the person and of their doings under the category of "same". It could be said that biometric control privileges the structure over the event by fixing the individual's identity at the risk of what Ricœur calls the "denial of change". But if a body (objectivised) remains well and truly the same, can the same be said of a subject and of the threat he potentially represents to a state? Is there not here a way of reducing a subject to inalterable characteristics which leaves little room for the appreciation of specific circumstances? What ultimately becomes questionable in the widespread use of biometric control procedures on all movements is the temptation to create dynamic parameters (the identity of an active subject) from stable data (those of his objective body) as if the future could always be deduced from the past.

There is also the risk of a loss of control over these data which gain value in travelling and in being saved. The sharing of these data with other states, which do not necessarily have the same scruples, nor the same concern for individual freedom, raises a number of questions. Too wide a circulation (in particular with private security firms) would render them indestructible. If biometric data were to prove both indestructible and permanent, they would condemn us to live in a fixed world with no refuge. A paradox in the age of globalisation and velocity.

Michaël Fœssel and Antoine Garapon

1. Definition given by Ayse Ceyhan during the Ihej/Esprit seminar, 20 March 2006.
2. See the position of the Cnil [French data protection authority] on the biometric visa experiment of 20 December (www.cnil.fr).
3. Decision of the House of Lords of 16 December 2004.

4. Rather it is biometrics that helps reconstruct life stories, as we shall see.
5. Ayse Cehan, “Securité, frontières et surveillance aux États-Unis après le 11 septembre 2001”, *Cultures et conflits*, 53, Autumn 2004.
6. Dominique Linhardt, Ihej/Esprit seminar, 3 April 2006.
7. A. Cehan, “Securité, frontières et surveillance aux États-Unis après le 11 septembre 2001”, art. cit.
8. M. Dobbs, “Homeland Security, New Challenges for an Old Responsibility”, Anser Institute for Homeland Security, March 2001.
9. Didier Bigo, “Gérer les transhumances. La surveillance à distance dans le champ transnational de la securité”, in *Penser avec Michel Foucault*, Paris, Karthala/CERI, 2005, pp. 130-160.
10. On this point, see the highly critical article by David Lyon “La frontière est partout : encartement, surveillance et altérité”, *Les Cahiers de la securité*, 56, 2005, p. 91-106.
11. See Giorgio Agamben, “Non au tatouage biopolitique”, *Le Monde*, 11 January 2004.
12. Agamben, “Non au tatouage biopolitique”, art. cit.
13.See Michel Foucault, *The Order of Things*, New York, Pantheon, 1971, where these formulae are used to characterise the system of natural history classifications of the 18th century.
14. Paul Ricœur, *Oneself as another*, Chicago, University of Chicago Press, 1992, trans. Kathleen Blamey, p. 3
15.*Ibid*., p. 141.

Revue des revues, sélection de janvier 2007

Michaël FOESSEL & Antoine GARAPON : « Biométrie : les nouvelles formes de l'identité» article publié initialement dans *Esprit*, juillet-août 2006.

Traducteurs :

Anglais : Ros Schwartz
Arabe : Anouar Moghith
Chinois : Yan Suwei
Espagnol : Claudia Riva-Palacio
Russe : Ekaterina Belavina