National Consultative Ethics Committee for Health and Life Sciences

OPINION N° 98

Biometrics, identifying data and human rights

Members of the Working Group:

Jean-Claude Ameisen

Sadek Béloucif

Pascale Cossart

Mireille Delmas-Marty

Chantal Deschamps

Chantal Lebatard

Pierre Le Coz

Philippe Rouvillois

Michel Roux

Maxime Seligmann (rapporteur)

Alain-Gérard Slama

Claude Sureau

Mario Stasi (rapporteur)

Persons heard:

M. Jean-Louis Bruguière

M. Vianney Dyèvre

M. François Giquel

Contents

I – A transformed approach to human identity

A) The supremacy of biometrics over other means of identification

B) "Ipseity" is being replaced by "sameness"

II – The power of biometrics: between progress and excess

A) The main purposes of biometrics

B) Risk of abuse

III – Privacy and otherness

IV - Recommendations

Identification of a person has always been founded on a few morphological parameters, among which facial recognition was indispensable. Photography became its most transferable trace. At the end of the 19th century, certain traits were even used to classify or predict types of behaviour.

The recently accelerated development of ever more sophisticated methods of physical identification, sometimes unbeknown to the person concerned, is fostering a growing collective temptation to improve security by increasing parametric precision.

The conflict between aspirations to security through constantly improved biometric identification and respect for human dignity inspired CCNE's self-referral on this matter.

What price must be paid to make life safer? Ethically, what is the best use that can be made of this "biometrification" of mankind? Are we not deluding ourselves when we think that each person's freedom can be protected by identifying others at a time when individual technical traceability is already anchored in the facts of everyday surveillance? It is true that biometric identification is not designed to reduce people to a set of identifiers. Its aim is to make sure that a person who claims a certain identity does exist. But in fact, the slippery slope leading from identification to identifying behaviour, and therefore personality, does appear to be a risk or even a natural inclination.

The three most worrying issues are therefore that identity checks might lead to monitoring behaviour, that data become interconnected and that they are acquired unbeknown to the person concerned.

I – A transformed approach to human identity

A) The supremacy of biometrics over other means of identification

Recognition of identity, so that a person's singularity can be claimed, is one of the fundamental human rights (in particular it is one of the rights of children recognised by the International Convention on the Rights of the Child). However, recognition of an individual by his or her name and possibly using a photograph is not longer thought to be sufficient.

With the passage of time and with advances in the means and the needs, the identifying elements (name, first name, plus information as to the village or region of origin, profession, physical features, etc.) are becoming more precise. The introduction of more scientific means of measurement providing more reliable identification has progressively modified our collective and individual relationships. We wish to be recognised in our personal singularity, we do not wish to be confused with others, but above all we wish to know with certainty if the person we are speaking to is the person he or she claims to be.

In today's world, such identification is achieved through an ever larger collection of ever more

sophisticated measurable parameters. They can be instantly and electronically checked through data banks so as to verify a claimed identity and to describe, if needs be, a pre-registered person. The combination of all this information provides an almost infallible result and encloses each of us within a well-defined framework. Society seems to be content with characterisation of a person by a set of data assembled in this manner. Due to mounting apprehension regarding security, in the wake of terrorist attacks among other reasons, the practice has recently escalated. This change in scale and pace in the progress of means of identification is in itself a reason for disquiet.

Identification by recognising morphological characteristics has made considerable advances: facial photographs and finger prints are now digitised which makes them easier to store and access. A collection of more or less reliable and more or less intrusive methods has been added to these traditional means of identification: hand geometry, venous networks of fingers and arms, recognition of the retina and its venous network and above all iris scan. The iris is very complex and for all practical purposes unique for each individual (the risk of error is estimated at 1:200bn); it is not modified by age, disease, or professional activities and cannot be erased. The iris can be recognised at a distance and without the person concerned being aware that this is taking place.

The growing use of means of identification by recognition of characteristic behavioural features (voice recognition, keyboard touch, gait) has ceased to be only used to describe an individual. They now seek to define the individual, to know more about who[1] he is, what he does and consumes. To the above must be added the proliferation of video surveillance systems, the location of people through their mobile telephones (or by the Paris underground's annual travelcard system for example) which, since they provide perfect traceability, can be viewed as relentless supervision of the freedom to come and go at will.

DNA testing methods are gaining a great deal of ground, perhaps too much. Of course, the genetic characteristics contained in the coding sequences are only stored and used for medical

[1] A recent European project included in the 6th Framework Programme (www.humabio-eu.org) aims to study the new physiological biometric parameters (records of electro-encephalograms, electro-cardiograms and electro-oculograms) by combining them together with traditional identification data so as to arrive at particularly reliable identification systems, and recording these characteristics using new wireless sensors representing a risk of stealthy detection. This project strikes us as worrying in that it also seeks to use these physiological parameters to verify the absence of recent intake of alcohol or drugs, or sleep deprivation in employees who are tasked with transporting funds, piloting aircraft, manipulating dangerous products either for recruitment purposes or as a permanent check on their vigilance status. The use of such methods for security purposes is of course only acceptable with the consent of those concerned and providing the laws on medical practices at place of work allow it, but more importantly security must be weighed against the degree of personal intrusion. The risk of making people the instruments of security is a matter of concern to occupational medicine which may be tempted to transfer onto a collection of measurable data the relationship with an employee, in the same way as medical practices giving more importance to imagery and figures than to people is a step on the way to dehumanising medicine.

purposes or scientific research, whereas the genetic "prints" used by the police and the law only involve the sex markers and the theoretically non-coding sequences. The theory supporting this distinction is perhaps mistaken and the non-coding sequences may well be the richest source for various kinds of information.

Do the various biometric data that we have just considered constitute authentic human identification? Or do they contribute on the contrary to instrumentalising the body and in a way dehumanising it by reducing a person to an assortment of biometric measurements? Is there not a possibility that this attempt to arrive at a biometric simplification, which cannot ever capture an individual's essence, could in fact lead to misrepresentation, to seeing nothing but the biometric persona, however scientifically determined?

They may reduce human beings to an accumulation of data and cartographic criteria, paradoxically at a time when biology is moving away to some degree from the reductionist and analytic approach and is seeking to apprehend systems holistically through an integration of all the properties of an organism or of a life form (integrative biology).

There is also the consideration that generalising these morphological identification processes could obviously lead to stigmatising certain people, such as those living with a handicap, or excluding those who cannot easily be measured.

B) "Ipseity" is being replaced by "sameness"

The above questions lead to a useful distinction, proposed by Paul RICOEUR[*]**.** In fact, the word "identity" applied to a human being can designate in French two different aspects of reality, which do not convey the same tension. The first meaning concerns the body objectively: through space and through the years, wherever life and the passage of time takes it, the body remains the same, despite the marks, lines and scars that time and events inflict. This first aspect of identity could be called "sameness". This can be captured by biometrics: from conception, with the help of genetic analysis, until death, through the use of identifying bodily data obtained by various means — in particular morphological characteristics and facial photographs.

The other reality is concerned with life's experience, with the life of a sentient and conscious human being. This is the "*self*" that the English language uses. To distinguish it from the first

[*] Paul RICOEUR, Soi-même comme un autre, (Oneself as another) Ed. du Seuil 1990, pp.39-54: "La personne et la référence identifiante ".

meaning, the term "ipseity" can be used, from the Latin "ipse", that is self as a reflective subject. This reality is of course subjective, but is important in ethical terms since it is what makes the exercise of freedom possible. Our perception of human dignity is inseparable from the inner biographic dimension that we call *ipseity*. From this viewpoint, it is the body as a subject — and not just the body as an object — that is in question, the body as it is experienced from the inside and not as it is seen from the outside. It is to *ipseity* that we refer our emotional experience and the intimate feeling that we remain the same from the beginning to the end of our lives. It is with this meaning that Ricoeur says of *ipseity* that it is "the individual's steadfast self throughout the vagaries of events constructing a life".

Nor is it in a body as an object but in the experience of their own flesh that men become aware of their vulnerability and of their mortality. They seek in a number of ways to protect their "ipseity", their personal identity, keeping its values intact. They do so in particular by creating and adopting within their life in society space for access to their inner selves, for privacy. The first of these is physical privacy, protected by the rules of modesty, although these rules may be broken in certain circumstances when care from family members or doctors demands it. Or again, sexual privacy which is open to partnership in certain circumstances. Beyond this inner physical circle, there are other protective areas since each community by inclination or common interest creates its own limits and defines an area of accepted internal communication and of controlled external communication. Each group has its own "secrets", which are in fact a condition of free communication.

The broadest group of all — barring the community of mankind — in today's society is the group represented by the State. It is generally accepted that in exchange for the services expected from it, the Sate recognises its own members with the help of external identifying data, which is in a way physical data made public, what we call the "civil status". The data are connected to the individual's own name. They identify within the public space each citizen by his or her "sameness" and can state "this is the person". But does it always respect the "ipseity" which underpins freedom? Does it not tend to dilute ipseity in a collection of digitised parameters?

When such data proliferate and diversify, when data bearing on physical intimacy and fragility are cross-referenced with data pertaining to other areas of life in society, revealed to other players through different data connected to various behaviours and collected for different reasons, there is legitimate reason to fear for the survival of the free space left to an individual, the individual's "ipseity". This is the basic ethical issue.

II – The power of biometrics: between progress and excess

A) The main purposes of biometrics

The diversity of identification methods is matched by the diversity of purposes. The uses that are made of identifying data must be classified according to their purpose:

- Public security in the broadest sense in the hands of recognised authority (justice, law and order,
- Public health,
- Medical and scientific research,
- Private (purely personal, collective within an organisation or business enterprise, for example).

These uses may be viewed as being in the service of the individual or to the individual's detriment, or for the benefit of third parties or detrimental to them, which may lead to at least apparent opposition between private and public interests.

Identity cards and passports are increasingly based on biometric and electronic technology in order to avoid fraud and identity theft and to provide authentication. But in what is now a globalised context, national regulations may be made totally ineffective, and therefore ignored, if countries are uninformed of each other's legislation.

The demands of the U.S. authorities that European airlines communicate over thirty items of identification — some of which openly seek to know "who you are" (food preferences, using a wheelchair, credit cards, etc.) — are more of a cause for concern.

Biometric techniques are also used in legal proceedings. Civil law courts use them in particular when filiation is disputed or needs to be established[*]. The absence, generally speaking, except in France and Belgium, of any supervision of test laboratories involved in such work, although offers abound on the internet, is also worrying.

Under criminal law, originally in France the only genetic prints that could be stored were those of people convicted of sexual offences, including some offences against minors. Recently however, the possibility of collecting and storing DNA samples has been extended to "any person who may plausibly be suspected, for one or several reasons, of having committed an offence", of which an exhaustive list includes "degradation, deterioration and threats against property". In many cases, it is difficult to claim that such an extension is required by reason of public security (is there any

[*] France is one of the only countries where biological expertise as regards filiation is under judicial supervision.

essential need to sample the DNA of people charged with destroying GMO crops?). If the end purpose is to make a start on generalised sampling covering the whole population, using as a pretext an infraction against any particular rule is quite unnecessary. As for any other enterprise but more so in this case, there must be a clear definition of purpose.

The management and supervision of a national health service requires the use of computerised identifying data. The French "carte Vitale" (a medical ID card) is designed to improve the continuity and quality of health care, this being one of the important factors in dealing with emergencies, and will be used to access the computerised personal medical data file for everyone which is currently planned. The nature of the identifying data which it could legitimately contain and which could make it into an authentic medicosocial ID document raises some delicate issues. Some masking procedures (and masking of the mask) should be authorised even though this may lead to a degree of loss of medical chances of recovery. The card should not bear any relation to the computerised identity card which is established — and must remain so — for the sole purposes of law and order and security. The medical Social Security number should not be used as the general identifying number which in particular gives access to medical files or to other privileged information.

As regards medical and scientific research, similar but even more significant problems arise with data collection, a practice which is undergoing unprecedented extension with the appearance of medical databanks by reason of the number of items that can be stored and the wide variety of uses they can be put to. The issue is not confined to biometrics as such but involves the integration if biological data into a complex system containing behavioural, psychological and other data. CCNE, in its Opinion n° 77, insisted on the need to anonymise even if it entails the loss of some scientifically useful data.

Identification and surveillance are omnipresent in the uses to which both private individuals and business concerns are putting biometrics at this time.

Site access control which used to be mainly focused on the presence or physical location of individuals is now extended to the use of computers.

Development of these techniques are not limited to uses involving third parties whose identity needs to be verified. Biometrics are intruding into everyone's daily life through a broad variety of tools, ranging from accessing safeboxes to starting motor vehicles and also involving certain facets of behaviour (for instance the kind of books consulted in a library or consumer habits in a

supermarket).

Altogether there is a great diversity in the use made of identifying data as regards both private and commercial transactions:

• On a personal basis in daily life.

• For reasons of public security, such as fighting bank card fraud.

• In the relationship between a company and its clients, both to identify them for security purposes and to facilitate their access to services.

• In the relationship between employers and employees, for access to premises or to organise employee databases (which are in fact prohibited).

There is reason to doubt whether a private company, which is not under the same kind of supervision as public bodies, should be allowed to demand certain intrusive biometric data with all the attendant risks, either when employees are first hired or during their working life with the company (risk of exclusion, discrimination and loss of privacy).

B) Risk of abuse

When data are collected, the purpose must be clearly and precisely stated, explained and justified, which implies that the authority or organisation which is proceeding with the collection must be precisely identified.

The securing of consent is an essential principle to observe when biometric data are collected. The principle is violated when identifying data are collected without the subject's knowledge (remote iris photography, remote electronic registration) or when consent is not required, as in England, to sample a hair, a fingernail or saliva. In France, although the need for consent to sample genetic material is included in article 16 of the *Code Civil* (Code of Civil Procedure) (and more specifically in articles 16.10 and 16.11), it was recently negated by a law to the effect that refusal to comply with a request for sampling is an offence. The very principle of consent is therefore overturned and normally this should encourage greater caution and more meticulous attention to the way in which samples are taken and identifying data are used and stored.

Strict respect for the purpose at hand is vital and any confusion between identification and information of a personal nature must be avoided. A considerable amount of data can be used for other purposes than those for which it was originally intended thus enabling pervasive and close supervision of people, their movements and activities.

In France, the time limit for storing genetic identification material is 40 years for convicted criminals and 25 years in other cases. The time limit is 100 years in England. Such interminable and

uncontrolled storage, without any possibility of removal if the person concerned requests it, is contrary to the principles governing the statute of limitations and amnesty. Furthermore, although proof given of guilt may justify the creation of some form of identifying databank of police records, there can be no justification for keeping such data when the samples concern people who were subsequently cleared of any wrongdoing.

If these principles are not followed, such practices are no longer concerned with respecting the purpose for which justification was given. They become simply storage of data "in case it comes in useful" but which make it possible to carry out discriminatory research, indulge in exclusion and sort subjects into groups for dubious reasons. The use of biometric data to identify ethnic minorities or their abuse for political purposes is a particular cause for concern. It is easy to imagine the use to stigmatise, exclude or even eliminate that totalitarian regimes might have made or could make with such instruments at hand!

The British police has a genetic database containing information on nearly four million people and in a recent enquiry, the Nuffield Council on Bioethics wondered whether it might not be more equitable to take DNA samples from all new-born British babies. On the other hand, in 2005 the European Parliament and a European Commission working group rejected the creation of a central biometric bank for passports belonging to all European Union nationals as contrary to the principle of proportionality of means.

The proportionality of means concept is an essential one since integrating personal data beyond what is really necessary for the stated purpose is clearly unethical.

This disproportion between ends and means highlights what is really at stake, i.e. intensified surveillance of human behaviour in the name of protection.

The validation of data must be meticulous since appeal against possible errors may be difficult. Similarly, access control to data must be extremely strict to avoid breakdowns in confidentiality, fraudulent theft and perversion of so-called sensitive data.

Finally, any collusion between public and private data represents a major risk and merging must be rejected out of hand. For instance, cross-referencing administrative and health-related databases could lead to serious discrimination in insurance or employment, in particular when people apply for work. Any doubts as to the seriousness of the issue can be dispelled by considering the systematic use of electronic search engines made by employers and recruiters.

Control of access to data and the risk of mergers are not confined to electronic databases. The situation is identical when data, frequently both public and private, are stored on electronic chips,

either externally and readable without contact or implanted in someone's body for all kinds of applications (checking on prisoners released on parole, security on public transport networks, access to discotheques, etc.).

The generalised use of RFID (Radio Frequency Identification) tags instead of bar codes has added a whole new and spectacular dimension to biometrification because of miniaturisation, infinite possibilities for remote data retrieval and low cost which has paved the way for a multiplicity of commercial uses[2].

Rigorous control of access is also required for medical or genetic databases. In this respect, CCNE mentioned in Opinion n° 77[*] the crucial role of the curator[**].

Extending such practices and thereby increasing the risk of abuse, leads inevitably to the need to set up bodies to verify the legitimacy of the data collection and of its declared purpose, respect of the stated purpose and the absence of any collusion constituting an obvious a threat to individual liberties. At the same time as these supervisory bodies are created, provisions should be made for instituting appeals procedures so that those concerned can have recourse, alas rather illusory in the event of covert data collection.

It is worth noting that the situation described above is obviously not limited by national borders and that protection would have to be transnational to avoid abuse and its consequences on personal liberties.

III - Privacy and otherness

Independently of the possibility of abuse, obviously reprehensible, biometry in itself entails the elevation of individual identification at the expense of societal values. Each individual must be tattooed and marked in the name of some principle of collective welfare. There is a gradual progression from identity as-an-individual-right to identity as-an-obligation or social duty. So-called collective security dictates its demands in the name of freedom.

---

[2] Michel Alberganti. Sous l'œil des puces. La RFID et la démocratie. Actes Sud, 2007

[*] Opinion n° 77 on Ethical Issues Raised by Collections of Biological Material and Associated Information Data : “Biobanks”, “Biolibraries”– Report – March 20, 2003 + Joint document by the French National Consultative Ethics Committee (CCNE) and the German National Ethics Council (Nationaler Ethikrat or NER) on Ethical Issues Raised by Collections of Biological Material and Associated Information Data: "Biobanks", "Biolibraries".

[**] The example of Iceland illustrates the risk of identification through cross-linked anonymised databases. For the whole of the Icelandic population there are three databases, all of them anonymised. The one containing medical data includes individuals post-mortem; the base containing geneological data gives an indication of profession and place of residence; the third and last contains genetic data. Cross-linking them allows identification and could give rise to filiation problems. This was one of the reasons for which Iceland's Supreme Court ruled that such a procedure would be unconstitutional. There are international repercussions as regards plans to produce vast European collections.

How does society itself react to the path it is now treading towards making everything safe and secure? It can be observed that although each one of us is willing to accept that others be marked in the name of collective security and reassurance, we like to reap the benefits but find the personal constraints distasteful. Everyone is afraid of everyone else; each one of us is in favour of setting up systems to enable identification and even authentication, but carps at the growing invasiveness of surveillance equipment into his own life, perhaps because the threat to individual privacy is becoming apparent. In this way, our innate impulse to bond with others is threatened either by more or less rational rejection or by compassion for this person that we are lucky enough not to be. Concern for others is not mediated by biometrics.

A society that prefers surveillance to vigilance in the name of growing demand for collective security is endangering individual liberties and rights to anonymity and confidentiality. Collecting identifying biometric data could involve a major breach of privacy and could therefore also be a violation of article 8 of the Convention of Human Rights which states that "Everyone has the right to respect for his private and family life".

Because of the paradox created between protection of privacy and encroachment on privacy, we are confronted with a kind of willing surrender of freedom. Surreptitiously, in the name of the security paradigm, our society is becoming accustomed to biometric markers and everyone seems resigned and even indifferent to being registered, observed, tracked and traced, often unwittingly.

The healthcare system can also be the unintentional source of medical information which could be put to use by the police or the judiciary. Generally speaking all administrative authorities are involved in the rapid expansion and the growing sophistication of electronic tools, not least the hospital system.

The fundamental issue is the interconnection of files, towards which computer systems naturally flow. Search engines work on that principle. It is not so much the parameters of biometrics that need watching as their interconnection which must be avoided at all costs, except by derogation allowed by judicial authority.

To sum up, the universal use of biometrics to define personal identity is spreading apparently unchecked and unimpeded, in the name of enhancing security supported by constantly advancing technology described as progress. The primary ethical issue is due to the belief that there is no alternative, although there has been no public and well documented debate on the potential dangers of this evolution and the abuse to which it could open the way.

It is a significant fact in this respect that the very people who are using these increasingly sophisticated and powerful techniques state, when asked, that there is no justification for them to set

any limitation on this activity themselves. They go so far as to call for public awareness on the subject, although in present circumstances this could only be the result of public debate unless the proliferation of technology and the use made of it for security reasons are allowed to encroach on privacy and the fundamental freedoms while public opinion remains indifferent.

It is the slippery slope inherent to biometrics which must motivate in depth reflection and reinforce the controls that a society aware of its obligations to its members must impose on itself.

This debate is not purely theoretical and has not been overtaken by events. There is in fact no guarantee that collective security will be better ensured in a world in which every form of exclusion is encouraged to the detriment of elementary solidarity. It is more than time to revert to the true purpose of biometrics so that technology can be a tool for real progress instead of an often inadequate and therefore counterproductive weapon.

In conclusion, CCNE is concerned by the tendency to generalise the collection of biometric data and the ensuing risks to individual liberties. The ever growing use of new technologies for the collection and transmission of personal data further increases the risk to individual liberties, which is even more cause for concern. Modern data acquisition methods are based on new generation electronic chips capable of collecting and storing large quantities of data and transmitting them by very efficient telemetric technology.

Despite apparent neutrality, data — in particular when physiological or psychological parameters disclosing identity, preferences or health status are included — can be misappropriated and used for abusive scrutiny of personal behaviours. Based for example on an analysis of the food preferences of travellers or of clients in a supermarket, conclusions can be drawn on their personal beliefs or on other facts for use in market surveys. This could happen without their knowledge, without their consent, to the detriment of their interests and therefore in conditions which are ethically unacceptable.

The risk of misappropriation is further aggravated by the possibility of transmitting the data using sophisticated telemetric technology which in no way guarantees confidentiality and gives no protection against illicit use. The biometric passport recently introduced in 27 European and American countries is an apt illustration of the risk of abuse of telemetry: convergent studies performed by companies engaged in electronic security and by the FIDIS Project (Future of Identity in the Information Society) commissioned by the European Union have shown that the confidentiality of data transmitted by the electronic chips in biometric passports is unreliable.

The generalisation, centralisation and disclosure, even accidentally, of biometric information of a personal nature must therefore be effectively controlled to prevent it from reducing the identity of citizens to a collection of instrumentalised markers and opening the way to surveillance in conditions which threaten privacy.

IV - Recommendations

In the light of the above analysis, CCNE recommends:

- Strict compliance with the purpose of each kind of data acquisition procedure and a clear definition of the organisations and authorities allowed to conduct it;

- Tight control over any systematic use of common identifiers under the supervision of the judiciary and CNIL (French Data Protection Agency). Prohibition of interconnection of databases designed for different purposes but with common identifiers. In particular, any regrouping of data liable to cause stigmatisation and discrimination in hiring decisions cannot be allowed since data rearranged in this way can only lead to the use of biometrics for exclusion, with particularly vulnerable people a preferred target. Enforcing this prohibition for databases in the hands of private organisations is admittedly a problem, but this should not prevent the principle from being plainly stated and making databases in public hands comply with it;

- Placing genetic identity databases under the authority of an independent judge, assisted if necessary by other judges;

- Strict implementation of rules applying to prior consent for data collection and effective control of any acquisition without the knowledge of those concerned;

- Solemn reaffirmation of the legitimacy of confidentiality protecting personal data, in particular information on physical and sexual characteristics or relating to an individual's family.

- Engaging in a thorough review of the use of electronic chips and telemetric transmission. The issue extends far beyond the limited scope of biometrics and requires the creation of an Agency to draw up a precise list of conditions in which the use of the technologies must be prohibited, whatever the circumstances;

- Remembering that the protection of those who are not included in any database must also be ensured, to avoid the paradoxical danger that their status becomes that of a "non-

citizen".

CCNE considers that it is essential to create an effective counterbalance to fight the excessive proliferation of biometrics. To be useful, measures protecting the freedom of citizens must be supported by independent structures designed to fight the possibility of technocratic, economic, police and political abuse in connection with the use of biometric data. CNIL, which is an example in France of a body meeting such criteria, should have its status and resources enhanced in order to improve its efficacy and independence. Coordination of such bodies at European level is also desirable.

Finally, CCNE suggests that a public debate be organised on the excessive generalisation of identifying data acquisition and its ethical repercussions. In order to encourage collective awareness of the nature of abuses and the need for effective control, the debate should be organised in cooperation with Committees on Ethics from other countries to provide the international dimension which is required for dealing with a problem so closely connected to human rights and dignities.

April 26, 2007

ANNEX I

PROVISIONS FOR THE COLLECTION OF GENETIC INFORMATION WITHIN THE FRENCH CRIMINAL JUSTICE SYSTEM

Articles 706-54 to 706-56 of the *Code de procédure pénale* (Code of Penal Procedure) set out rules for the operation of the central national computerised genetic fingerprinting system ***(fichier national automatisé des empreintes génétiques - FNAEG)*** designed to identify offenders.

The genetic fingerprint database is supervised by an independent *Magistrat du Parquet* (part of the public prosecution service, but not in the hierarchy), nominated by the *Garde des Sceaux* (Minister for Justice) for a period of three years. He is assisted by a committee of three members nominated in the same way. The *Magistrat* and the three members have permanent access to the database. The *Magistrat* may order any measures required for supervision, e.g. requisition or copies of data. These powers are exercised independently of those granted to the *Commission Nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Agency).

PERSONS CONCERNED

- Genetic fingerprints are sampled from convicted criminals and also persons against whom serious or converging evidence indicates that there is a probability that they may have committed one of the offences listed in article 706-55 of the *Code de procédure pénale.*

"The national computerised genetic fingerprinting system centralises genetic traces and prints concerning the following infractions:

1° Infractions of a sexual nature covered by article 706-47 of the code and the offence covered by article 222-32 of the Code Pénal;

2° Crimes against mankind and crimes and voluntary attacks on a person's life, torture, barbarous acts, voluntary violence, threats against the person, purchase and sale of drugs, attacks on personal freedoms, trafficking in human beings, proxenetism, exploiting mendicity of minors and putting them at risk, as covered in articles 221-1 to 221-5, 222-1 to 222-18, 222-34 to 222-40, 224-1 to 224-8, 225-4-1 to 225-4-4, 225-5 to 225-10, 225-12-1 to 225-12-3, 225-12-5 to 225-12-7 and 227-18 to 227-21 of the Code Pénal;

3° Crimes and offences related to theft, extortion, embezzlement, destruction, degradation, deterioration and threats against property , as covered in articles 311-1 to 311-13, 312-1 to 312-9, 313-2 and 322-1 to 322-14 of the Code Pénal;

4° Attacks on the fundamental interests of the nation, acts of terrorism, counterfeiting the currency and association of wrongdoers as covered in articles 410-1 to 413-12, 421-1 to 421-4, 442-1 to 442-5 et 450-1 of the Code Pénal;

5° Crimes and offences covered in article 2 of the law dated May 24, 1834 on the possession of weapons or munitions for warfare, article 3 of the law dated June 19, 1871 which abrogates de decree dated September 4 1870 on the manufacture of weapons of war and articles 24 to 35 in the decree dated April 1939 regulating equipment, weapons and munitions for warfare;

6° Offences of receiving or laundering the product of one of the offences listed in 1° to 5° above, as provided by articles 321-1 to 321-7 and 324-1 to 324-6 of the Code Pénal."

- Genetic print sampling is also performed on persons for which there are one or several plausible reasons to suspect they may have committed a crime or offence.

THE REQUIREMENT FOR CONSENT AND SANCTIONS FOR REFUSAL

- Consent is required for samples taken from the following persons:

- Persons convicted of one of the offences mentioned in article 706-55 (706-54 para. 1)
- Persons against whom serious or converging evidence indicates that it is plausible that they may have committed one of the offences mentioned in article 706-55 whose data are also kept in the database (706-54, para. 2)
- Persons for whom there are one or several plausible reasons to suspect that they may have committed a crime or offence, the data are included in the database, but the prints cannot be kept. (706-54, para. 3).

- However, **refusing to submit to biosampling** is an offence as described by article 706-56, II° CPP (since the law known by the name: "Perben II", dated March 9, 2004. The sanction differs depending on whether the author was convicted for a misdemeanour (one year of prison detention and a 15,000 euro fine) or for a crime (two years in prison and a 30,000 euro fine) as provided by article 706-56.

SAMPLING AND COMMUNICATION OF SEALED SAMPLES

Sampling and collecting biological traces and specimens is performed by a police officer. The officer in charge of the procedure may request the assistance of a qualified and authorised person. Traces are collected by investigators as part of the preliminary investigation or in flagrante delicto, or following a court order. For persons covered by paragraphs 1, 2, and 3 of article 706-54 (convicted or suspected persons), the police offer in charge of the investigation takes the biological sample or requests that this be done. The officer may verify or request a subordinate to verify that the print is not already registered before proceeding. (Article 706-56, I).

When the sampling procedure was not performed during investigations, prior enquiry or trial, it is performed for convicted offenders within one year of serving the sentence, at the request of the *Procureur de la République* or the *Procureur Général*. (public prosecutors, appellate and first instance). (Article R. 53-21).

The sealed samples are sent for storage to the central department for the conservation of biological samples, by decision of the Prosecutor, the police officer or the investigating magistrate. (Article R. 53-20).

CONTENTS OF THE DATABASE (FNAEG)

Article 706-54 para. 5 CPP states that *"genetic fingerprinting evidence kept in the database must contain on non-coding deoxyribonucleic acid (DNA) segments, except the segment corresponding to the sex marker"*.
It is not in fact possible to extract from so-called "non-coding" DNA segments physiological, morphological or hereditary information, apart from the sex markers. The intention therefore in excluding the use of "coding" segments, is to exclude from the automated database sensitive data on physical characteristics or genetic anomalies.

Article R. 53-13 states that the number and nature of the non-coding DNA segments used for genetic identification are stipulated by interministerial order. Thus, it is article A. 38 CPP which sets out the table of segments which can be used, according to the international nomenclature.

Also noteworthy is that the database stores not only traces and collected samples under seal but also the results of tests performed using the samples.

CONSERVATION AND ERASURE OF DATA

Prints sampled on persons against whom serious and converging evidence indicates that there is a probability that they may have committed one of the offences covered in Article 706-55 are erased by order of the *Procureur de la République* acting either *ex officio* or at the request of the person concerned, **once conservation appears to be no longer necessary for the purpose of the database**. The *Procureur de la République* informs the person concerned of the follow-up given to his or her request and if erasure was not ordered, the person concerned may refer to the *Juge des Libertés et de la Détention* (judge for imprisonment and release), whose decision may be referred to a special court of appeal (*Président de la Chambre de l'Instruction*). (706-54 para. 2 and R. 53-13-1 to R. 53-13-6).

In any event, they may not be kept beyond **twenty-five years** starting from the request for registration, unless their erasure is ordered before that time period has elapsed as provided by articles R. 53-13-1 to R. 53-13-6. However, if the case of the person concerned was dismissed, quashed, or gave rise to release or acquittal exclusively grounded on the existence of mental disorder by implementation of the provisions of the first paragraph of Article 122-1 of the *Code Pénal*, the *Procureur de la République* so informs the database administrator and the data are then kept for forty years from the date of that decision." (R. 53-14, para 2).

Biosamples from other persons many not be kept beyond a period of **forty years** from either the request for registration or from the day when the sentence became final or, if that date is unknown to the database administrator, from the day the sentence was passed, when the evidence is derived from the results of genetic identification on biosamples from persons convicted of one of the offences covered in Article 706-55. (R. 53-14, para. 1).
At the end of the forty years, the evidence is destroyed.
(Article R. 53-20).

Information transmitted to the central department can be computer processed as provided by law n° 78-17 dated January 6, 1978 on Data Processing, Data Files and Individual Liberties. Computer processing cannot, under any circumstances, contain the results of genetic identification tests.
(article R. 53-20)

There are no provisions as regards the FNAG or concerning amnesty or rehabilitation for the destruction of sealed evidence when a convicted person has been granted amnesty or rehabilitation.

****

ANNEX II

THE SITUATION IN THE UNITED KINGDOM

Data bases are governed by ordinary law and it is expressly accepted that the European Convention on Human Rights and Article 8 in particular are accepted as its source.

Through the 1998 Human Rights Act, the European Convention was incorporated (to some extent) into British law. Authorities are bound to respect the "Convention rights"; legislation posterior conflicting with "Convention rights" must be left aside; anterior legislation (i.e. Acts of Parliament) must be interpreted insofar as possible to be compatible with the Convention; when it is not possible for an Act of Parliament to be interpreted so that it is compatible with the Convention, the Courts must apply it but must issue a "declaration of incompatibility" which paves the way for accelerated procedure in order to amend the Act (if the Government so wishes).

The question arose as to whether Article 8 of the European Convention applies to the conservation of biometric data.
The question was examined by the House of Lords (R (S) v Chief Constable of South Yorkshire Police [2004] 1 WLR 2196) which ruled as follows:
(i) Simple retention (as opposed to disclosure) of personal data complies with Article 8;
(ii) For the majority, the retention of DNA to identify a person, without the possibility of obtaining other information on that person, is in breach of Article 8;
(iii) But (unanimously), even if the retention of DNA samples is relevant to the rights set out in Article 8 § 1, the purpose for which the samples were stored requires justification.

The 1998 Data Protection Act (DPA) restricts the registration of personal data and imposes further restriction on the registration of so-called sensitive personal data.

> Section l:
> "Personal data" means data which relate to a living individual who can be identified-
> (a) from those data
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;
>
> Section 2:
>
> "Sensitive personal data" means personal data consisting of information as to-
>
> (a) the racial or ethnic origin of the data subject,
> (b) his political opinions,
> (c) his religious beliefs or other beliefs of a similar nature,
> (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
> (e) his physical or mental health or condition,
> (f) his sexual life,
> (g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Those who process the sensitive personal data must respect a number of "data protection principles" which are contained in the first four schedules of the Act. Those responsible for processing data in breach of these principles are liable to be proceeded against but a large number of exceptions are listed in attenuation of the demand to respect the "data protection principles" or in some cases, some of these principles, as for example the prevention or detection of crime or the collection of tax.

The 2004 Human Tissues Act restricts the storage and use of human tissues without appropriate consent. Section 45 defines the limits for the use and storage of DNA. It states that:

(1) A person commits an offence if

(a) he has any bodily material intending-

(i) that any human DNA in the material be analysed without qualifying consent, and
(ii)that the results of the analysis be used otherwise than for an excepted purpose,

(b) the material is not of a kind excepted, and

(c) he does not reasonably believe the material to be of a kind so excepted.

(2) Bodily material is excepted if -

(a) it is material which has come from the body of a person who died before the day on which this section comes into force and at least one hundred years have elapsed since the date of the person's death,

(b) it is an existing holding and the person who has it is not in possession, and not likely to come into possession, of information from which the individual from whose body the material has come can be identified, or

(c) it is an embryo outside the human body.

(3) A person guilty of an offence under this section-

(a) is liable on summary conviction to a fine not exceeding the statutory maximum;

(b) is liable on conviction on indictment-

(i) to imprisonment for a term not exceeding 3 years, or

(ii) to a fine, or

(iii) to both.

(4) Schedule 4 (which makes provision for the interpretation of "qualifying consent" and "use for an excepted purpose" in subsection (1)(a)) has effect.

(5) In this section (and Schedule 4)-

"bodily material" means material which-

(a) has come from a human body,
(b) consists of or includes human cells;

- "existing holding" means bodily material held immediately before the day on which this section comes into force.

"Use for an excepted purpose" in Schedule 4 includes inter alia:

(a) the medical diagnosis or treatment of the person whose body manufactured the DNA;
(b) purposes of functions of a coroner;
(c) purposes of functions of a procurator fiscal (Scotland);
(d) the prevention or detection of crime;
(e) the conduct of a prosecution;
(f) purposes of national security;
(g) implementing an order or direction of a court or tribunal.