

Presidenza del Consiglio dei Ministri



**THE IDENTIFICATION OF THE HUMAN BODY:
BIOETHICAL ASPECTS OF BIOMETRICS**

26th November 2010

PRESENTATION

The document addresses the subject of “biometrics”, that is, new techniques for the identification or `measurement` of the human being through the detection of specific physical and behavioural characteristics which are reproduced in the form of mathematical sequences and stored in electronic databases. The text begins with a synthetic description of the state-of-the-art in terms of science and technology it pinpoints the biojuridical and bioethical issues, within the context of a reflection on the body and on the need for safety and privacy.

The NBC focuses on the advantages offered by the use of these new technologies for the safeguarding of public order within interpersonal relationships and highlights the possible risks arising from uncontrolled misuse, with particular reference to discrimination, stigmatization or social exclusion. The NBC expresses several recommendations for the protection of the individual (the use of biometrics only for reasons of necessity, used with proportionality, with informed consent and recognising the right of access to data and the so-called 'right to oblivion') and for the regulation of biometric applications, internationally and nationally.

The document was drawn up by the coordinators of the working group, Profs. Salvatore Amato and Cinzia Caporale, with the collaboration, for the scientific and technical aspects, of Dr. Mario Savastano, Senior Researcher at the CNR in Naples and an expert in this field. The group was attended by Profs. Luisella Battaglia, Riccardo Di Segni, Giancarlo Umani Ronchi, Monica Toraldo di Francia, Grazia Zuffa. The document was unanimously voted by: Profs. Salvatore Amato, Luisella Battaglia, Adriano Bompiani, Stefano Canestrari, Cinzia Caporale, Antonio Da Re, Lorenzo d'Avack, Riccardo Di Segni, Emma Fattorini, Silvio Garattini, Marianna Gensabella, Claudia Mancina, Assunta Morresi, Demetrio Neri, Andrea Nicolussi, Laura Palazzani, Vittorio Possenti, Rodolfo Proietti, Lucetta Scarraffia, Monica Toraldo Di Francia, Giancarlo Umani Ronchi. Profs. Francesco D'Agostino and Romano Forleo absent at the plenary meeting subsequently expressed their support.

The President
Prof. Francesco Paolo Casavola

DOCUMENT

1. Preamble

The identification of human beings is a cognitive and psychological fundamental requirement demonstrated without exception in every society. It has assumed increasing importance, especially in light of security needs in interpersonal relations and in economic relations, raised in a comprehensive way in all countries and at all levels. In order to automate the identification procedures or identity verification, in recent years a specific technical and scientific discipline has been established called "biometrics" which aims to achieve these goals through the assessment of the physical and/or behavioral characteristics human beings¹ acquired by electronic sensors, developed by special mathematical algorithms and converted into numerical models. The characteristics should be easily measurable, specific to a particular person, or unique and unambiguous in the face of wide variability in the population, and must remain as constant as possible over time. Technological development has made the resources and tools identifying highly sophisticated, complex and efficient, increasing the opportunities and benefits, but at the same time multiplying the opportunities for social control.

The body has assumed the role of a real *password*² that is to say, a living code of recognition that integrates and interacts with the world of machines. The uniqueness of our individual characteristics can be recognized from what we are (face, fingerprints, DNA, etc.), and what we do (voice, gait, signature, etc...). Both characteristics can also be associated with what we *have* (passport, credit cards, memberships, etc.) or *know* (PIN, access codes, etc...).

None of these elements for detection alone constitute individually a bioethical problem, but associated with each other and linked systematically and steadily through computer networks, they could profoundly affect the ways of appearing and acting of each individual, or even become an instrument of exclusion and stigmatisation. The reference is to possible misuse or real abuse as biometrics interprets the human body as a mere source of information that can be treated at times without the knowledge of the people concerned; all this for purposes other than those stated and carried out by different parties sometimes unknown or unknowable to the person involved. The problem of the protection of individual identity therefore takes on aspects that go far beyond the traditional limit of the respect of privacy, as there is the real risk of placing the identification processes, processes consequently of social and existential importance, outside the control of individuals.

In fact, if in the past biometrics had a clearly defined role and was limited to the investigative and juridical context, currently the areas of application involve increasingly large and important spheres of social life: from access to certain places, to enjoyment of particular services, traceability, with an exponential technological progress in many fields (Health protection, health care fraud prevention, protection of confidential medical information, monitoring access to restricted areas and efficiency in trade, financial and military security,

¹ There are also applications dedicated to biometric identification of animals.

² A. Davis, *The Body as Password*, On Newsstands Now, issue 5.07, July 1997 (Wired), available (from 21/11/10) at: <http://www.wired.com/wired/archive/5.07/biometrics.html>; A.K. Jain et al, *Biometrics: personal identification in networked society*, Kluwer Academic Publisher Group, 1998.

border control and migration etc.) and a corresponding expansion of the market. An additional role of biometrics, which is currently marginal and in any case outside the classical definition of the scope of application of these technologies, may be constituted by a contribution to the diagnosis of diseases.

The advantages in these sectors seem quite obvious as biometric data are harder to forge, easier to use and impossible to forget or lose. The user therefore has a vested interest in a progressive increase in the use of biometrics, demanding however at the same time, even in terms of scientific and technological innovation, reliable methods of recording biometric data (*accountability*), and transparent data management systems, that are efficient and guaranteed (*reliability*).

The social requirement of *accountability* and *reliability* is closely related to governance issues in relation to the management and control of data collected nationally and internationally. The natural flow and extraterritorial nature of the information radically alters the guarantees offered by traditional forms of administrative and judicial protection with regard to the safeguarding of personal freedoms and privacy, and presents interrogatives all the more urgent the more rapid the movement of information and the intensity of trade.

There is also a widespread concern that an identification system that is more and more systematic, automatic and pervasive is likely to affect behaviour: the individual runs the risk of assuming social importance only for the traces he leaves. This relates above all to the quantity and manipulability of these traces and their "portability" in the form of a mathematical string. In addition, if it is possible to replace a credit card or request correction of erroneous data in an identity card with relative ease, it is not as easy to dispose of an algorithm that represents the body and is contained in many electronics archives. Furthermore, not only physical data can be acquired stably, but they can also be linked with personal data such as health status, tastes, habits, and for purposes that are public or private, social or individual, often unrecognized and in the absence of explicit consent. What is apparent is the technical feasibility of new and subtle forms of control, and consequently, in some respects, even the affecting of personality, at least to the extent that it may be claimed as a duty to "remain" in a biometric system and a personal responsibility for the "maintenance" of biometric data (paragraph 4.2).

Bioethical reflection is faced with a technology of fundamental importance for the quality of life of people and the stability and security of economic and sociopolitical relations, it can not help but wonder about how this technology affects the explication of spheres of autonomy and reduces the areas of non-interference. A society that is able to record and store a large part of individual behaviour and choices that individuals make every day could lose the right balance between freedom and security. If the certainty and security that biometrics will strengthen and improve, constitute the fundamental elements for the exercise of freedom and several fundamental rights, systematic and constant control of an ever-increasing and undetermined number of behaviours could in fact represent a discreet, but not less insidious form of biosurveillance, to the point of imposing, to be socially accepted, the "forced" taking of an identity. How desirable is the building of a world without oblivion? A world where everyone has value even based on the quantity of "traces" that are stably and definitively entrusted to the algorithms of biometric mechanisms?

Will identity as an individual right to guarantee the exercise of fundamental freedoms gradually be eroded by increasing duties of identification? Is there a

right to *biometric anonymity*? To what extent can we ensure the secrecy of personal identity?

2. Introductory notes and status of biometric data

2.1 General taxonomy

Biometric characteristics represent the biological or behavioural features of an individual from which the information used for biometric recognition can be extracted.

The essential properties that biometric features should have for the purpose of biometric authentication are:

- *universality*: each individual should have the biometric feature;
- *distinctiveness*: the element of biometric reference should allow to distinguish, to the greatest extent possible, each individual from all others;
- *permanence*: the element used for biometric analysis should guarantee over a period of time a certain level of recognition;
- *collectability*: the biometric feature should be quantitatively measurable and inserted into a stable system of detection.

Assuming that 1) any biometric process begins with inclusion of the particular subject in the system and that 2) from the subject's biometric features a mathematical model called *template* is generated; for biometric technologies, there are two operating modes that have a completely different value both from a technological and legal point of view:

A. the "Identification" mode attempts to assign an identity to a given subject through a "one-to-many" match comparison technique between the *template* of the biometric traits of that subject, which is generated at the time of the transaction, and all the *templates* present in a given archive and related to a set of subjects. Generally, each *template* contained in the archive corresponds to an identity, and therefore discovery of the *template* which, within a tolerance band, has the highest similarity, is equal to identification of the subject. Even if the biometric data of the subject were not contained in the archive, this would still be of some use as it could be excluded, within a reasonable margin of error that the given subject belongs to that specific set of subjects;

B. the "Identity Verification" mode attempts to determine whether a person is who they claim to be. The procedure consists in a "one-to-one" match comparison technique between the *template* of the biometric features of that subject, which is generated at the time of the transaction and a specific *template* present in a given archive. For example, by keying in a PIN the subject indicates to the system the *template* already present in the archive with which to make the comparison that will verify whether or not the person is who they claim to be. The "Verify Identity" mode can also directly carry out through comparison of the *template* created at the time of the transaction with the one stored in an electronic map in the possession of the person concerned, all to the benefit of an increased level of the protection of personal data as the subject does not have to deposit the *template* regarding biometric features in an archive.

Other distinctions that are commonly made in the sphere of biometrics, with important consequences in ethical and legal terms, classify application contexts as³:

- *manifest or hidden*: Depending on whether or not the user is aware of being subjected to a biometric identification system (most of the applications are manifest, however some applications, related to police investigations or the maintaining of public order, may be hidden);
- *characterized by accustomed or unaccustomed users of biometric technology*: according to whether the user population has or lacks experience in the use of biometric systems;
- *attended or unattended*: according to whether the biometric system is staffed or not, supervised or assisted by an operator;
- *situated in standard environmental conditions or not*: depending on whether the system is or is not likely to operate in standard environmental conditions (i.e. with temperature, humidity and lighting values that are within a certain range of tolerance);
- *public or private*: depending on whether the users of the system are in public areas (e.g. an automatic border control) or in private areas (e.g. access to the home);
- *open or closed*: depending on whether the acquired biometric data reside solely in the logical or geographic place of the application or whether they can be exported to other applications.

Further classifications also include: (a) the distinction between *cooperative or non-cooperative* applications, depending on whether or not the consent and cooperation of the actual subject is required to carry out the process of authentication/identification; (b) the distinction between *positive* biometric identification, in which the person provides proof biometric of actually belonging to a given set (e.g.: to belong to the group that has to collect a pension), and *negative* biometric identification, in which the subject states according to their biometric credentials that they do *not* belong to a given set (e.g.: they are not among those who have already collected their pension).

Finally, some experts distinguish between biometric technologies that allow both identification and verification of identity, and others that allow only the verification of identity, such as the one based on recognition of hand geometry. The difference lies mainly in the inherent capacity of the biometric feature examined to distinguish between users. The parameters measured in hand geometry do not vary significantly in the population: this means that it is impossible to carry out identification, but it does not preclude verification processes (indeed, this is the method of choice for verification).

2.2 Stages of a biometric process and potential errors

In general, the stages of a biometric process are the following⁴:

³ J. Wayman et al, *Biometric Systems, Technology, Design and Performance Evaluation*, Springer, 2004.

⁴ Idem.

- *acquisition of the biometric feature*: in this phase, the user presents their biometric credentials to the system (that is, their biometric characteristics) through a *sensor*;

- *transmission of data*: the acquired data is transmitted from the sensor to other parts of the biometric system for further processing; the sensor may be near or at some distance from the rest of the system and it is important to assess this parameter in terms of the risks of vulnerability of the system (misappropriation of data captured along the way), and also for the possible deterioration of the quality of the information;

- *the processing of data*: in this phase, data are prepared for the subsequent stages of the biometric process; a crucial operation that is completed at this stage is the generation of the *template*, that is to say, the mathematical model corresponding to the biometric data acquired;

- *storing the template*: during registration in the system (*enrollment*), the *templates* are stored within the system for subsequent activities of comparison of data;

- *comparison*: the *template* presented at the time of the transaction is compared, in terms of the measurement of similarity, with one (verification mode) or more (identification mode) stored *templates*;

- *validation / matching*: on the basis of measuring acceptability against a preset threshold value, the system can validate a "Verify Identity" or, in identification mode, generate a list of possible candidates characterized by a "*matching*" score; the system assigns the person in the transaction the identity of the candidate with the best "matching" score.

Performance of a biometric system is evaluated on a statistical basis and is a function of a great number of parameters. Like any system of statistical comparison, biometric identification includes margins of error whose magnitude depends on the type of biometric feature used⁵. Basically, changes in environmental conditions, registration, and data acquisition, as well as physical changes (temporary or permanent) or the time between *enrollment* and the biometric transaction play a key role by reducing the chances of recognition.

Some important parameters that measure the accuracy of a biometric system are⁶:

- FAR (*False Acceptance Rate*): false acceptance rate, which denotes the number of times a system provides an inappropriate indication of exceeding the threshold value of "similarity" between the acquired data and the stored data; in a system with a high value of FAR, there is an increase in the possibility of granting access to a place or to a service to an impostor;

- FRR (*False Rejection Rate*): false rejection rate that denotes the number of times that the system provides an inappropriate indication of failure to exceed the threshold value of "similarity" between the acquired data and the stored data; in a system with a high value of FRR, there is an increase in the

⁵ For example, errors made by a system for face recognition are usually higher than those found in systems based on fingerprint or iris recognition.

⁶ See, for example, Encyclopedia of Biometrics, S.Z.Li editor, A.K.Jain Editorial Advisor, Springer Science + Business Media LLC, 2009; R. Bolle et al., Guide to Biometrics, Springer-Verlag New York Inc., 2004; A. J. Mansfield, J. L. Wayman, Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01, August 2002, available (on 21.11.2010) at: www.cesg.gov.uk/policy_technologies/biometrics/media/bestpractice.pdf.

possibility of wrongly denied access to a place or service to a user who is however duly authorized⁷;

- ERR (*EER, Equal Error Rate*): the values of FAR and FRR describe two curves that depend on the threshold value of the biometric system. The point of intersection between the curves of FAR and FRR (where the two error rates assume the same value) gives the EER value, which, is essentially a measure of the global accuracy of a biometric system, it can be very helpful in determining which system is more appropriate in a given scenario.

For operational purposes, it is clear that to achieve high levels of safety in applications it is necessary to pursue a low FAR (in this case, in fact, the main concern is that the system will not improperly accept unauthorized individuals). However, by setting a stringent threshold of acceptance of biometric credentials, there may be a significant rejection rate (many people may be excluded from access to a place or a service). Similarly, if the imperative were the smallest possible rejection rate (FRR), for example, to facilitate quick access to a large number of users, the system should be designed so as to significantly reduce the acceptance threshold value. However, this of course, would cause an increase in the rate of undue acceptance FAR and a consequent decrease in the level of security.

It is clear that, the search for the optimal threshold value that allows an effective balance between FAR and FRR is one of the major difficulties faced by managers of authentication systems based on biometric technologies.

Finally, in a concise overview of the parameters that characterize biometric systems one should consider that a fraction of users may be unable to register in a given biometric system or, even if registered, could subsequently be unable to complete a biometric transaction. The *Failure To Enroll Rate - FTER* and the *Failure To Acquire Rate - FTAR* correspond to these two possibilities and are closely connected to concepts of accessibility and usability of biometric systems which, as will be shown later in this document, are two key elements in the overall assessment of a biometric system.

2.3 The most widespread biometric technologies

The most common biometric technologies are based on the recognition of:

- fingerprints;
- facial characteristics;
- hand geometry;
- the vascular structure of the palm and dorsum of the hand;
- voice characteristics;
- iris patterns;
- the vascular structure of the retina;
- signature dynamics;
- keystroke dynamics;
- DNA⁸.

⁷ In practice, this type of error is the most common and, unfortunately, creates frustration and distrust of biometric technologies by users.

In terms of research, various other biometric technologies are being studied. For example, presently under verification is the potential offered by systems based on recognition of ear morphology and in the context of assessment of behavioural biometric characteristics, systems for the recognition of gait.

3. The disciplinary context of biometric technologies

The study of biometric technologies involves interdisciplinary knowledge that may be collected, in extremely general terms, in the following list:

- Electronics;
- Computer Science;
- Statistics;
- Medicine;
- Psychology;
- Ethics;
- Law.

As can be seen from the list, many of the subject areas listed do not come under a purely "technical" dimension. Their contribution becomes very significant when biometric applications pass from an experimental laboratory phase to implementation in real operating conditions. All experiences at international level have also clearly highlighted the dangers arising from a lack of consideration of medical, psychological, social and ethical and juridical aspects of biometrics.

3.1 Biojuridical profiles of biometric technologies

On the assumption that 1) the context of biometric applications is fairly large, 2) there are substantially different views on the applicability of biometric systems depending on the social and geopolitical context, and 3) the regulations especially regarding the protection of personal data is constantly evolving, it can be said that certain parameters in principle, closely related to the juridical context of protection of fundamental freedoms, govern the applicability of biometric systems. First and foremost, it should be remembered that Article 10 of the Convention on Human Rights and Biomedicine include respect of the private sphere in relation to private health information (art. 10). In addition, the Charter of Fundamental Rights of the EU, art. 8 (*Protection of personal data*) clearly indicates some basic guidelines under which "1. Everyone has the right to protection of personal data concerning him. 2. Such data must be processed fairly for specified purposes and subject to the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access data concerning them and to have it

⁸ DNA analysis has recently been admitted to the biometric technologies which are at the attention of the sub-committee of ISO standards (ISO / IEC JTC1 SC 37 "Biometrics") although, unlike all the other biometric technologies, at least for the moment, DNA analysis does not allow authentication in real time. The latter criterion is not covered in the canonical definition of biometric technologies and therefore does not prevent to include DNA analysis among them.

corrected. Compliance with these rules shall be subject to the control of independent authorities".

Faced with this horizon, which is still subject to definition, the law has developed a comprehensive framework of legality around the need to guarantee the right to privacy through compliance with certain fundamental values in the light of articles 3 and 11, of the Code regarding protection of personal data (Legislative Decree. June 30, 2003, n. 196), as well as of art. 6 of Directive 95/46/EC:

- *proportionality*: the context of biometrics should be characterized by appropriately weighing up the relationship between the sacrifices imposed on personal freedom and the existence of specific security requirements. In general, the prevention of potentially hazardous conditions, both for individuals and for society, is considered a sufficient factor for the implementation of a biometric system, in the event that the same results can not be achieved in another way and with the same efficiency. In other words, the principle of proportionality is a basic principle in EU legislation and is underlined by numerous regulatory documents. It is therefore considered a crucial element in the choices regarding the applicability of biometric systems, made by the various national data protection authorities;

- *necessity*: the context in which the biometric application is implemented does not allow the resorting to other types of less invasive and equally sensitive technologies, able to achieve the same results offered by biometric technologies.

Proportionality and *necessity* must be assessed in relation to the *objectives* pursued, with particular reference to the context in which the data is entered and processed, and the *pertinent* relationship between ends and means.

One must bear in mind that respect for identity constitutes one of the fundamental human rights. Dignity and personal integrity are connected to identity. Both of which presuppose the singularity of each individual, the law must not only take account of this but also allow its greater expression in the variety of life contexts. Quoting Paul Ricoeur, Opinion No. 98 of 26 April 2007 of the *Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé* on the subject of "*Biométrie, données identifiantes et droits de l'homme*", he points out that identity is formed by two inseparable elements: the exteriority of the body, "mêmeté," with which we come into physical contact with others and with the world around us, and the inner biographical dimension, «ipséité», which expresses our deepest values, those that give meaning to life and around which freedom is built. The NBC agrees with this perspective. If juridical experience is based on the recognition and protection of the immediacy of physical fact, it is to permit the expression and realization of the intangible element of interiority. So in addition to the obvious benefits for social security, any improvement to the means of identification constitute abstractly also an increase in the opportunity of enjoyment of fundamental rights and the ensuring of protection of subjective positions: from the need to access and use your current account, your car, your plane ticket, to the opportunity to demonstrate participation or non-participation in a given event. Nor should it be overlooked that, in some respects, biometric data could get round the requirement of communication of highly personal information as is foreseen by current identification documents (e.g.: place and date of birth, sex, marital status, etc..),

or in another context, your health data (e.g.: infectious diseases), therefore improving the degree of confidentiality of those involved.

However, a risk not to be ignored is, that in other respects, biometric data reveals information in excess and is used for purposes that go beyond the intended purpose of authentication, resulting in a specific phenomenon which in jargon is defined *function-creep*, or "the exploitation of data"⁹ or undue expansion of the use of data. For example, DNA, in addition to genetic identity, captures information on the susceptibility to diseases in general and on individual phenotype, the method of recognition of the retina the part of the eye which is characterized by high vascularity may indicate the presence of hypertension or diabetes, iris analysis can show the use of alcohol or drugs, temperature or some characteristics of particular areas of the face can detect psycho-physical or even pathological condition. It is possible that these data are captured and then released, unknown to or even against the will of the subject. This can lead to a distorted movement of the information that, in extreme cases, could produce potentially uncontrolled disturbing scenarios.

A further source of concern arises from possible aggregation of data. Through the overlapping of biometric data with other information (such as medical, financial or behavioral information) it is possible to imagine their centralized and combined use for so-called *profiling*. Profiling can be defined as the act or process by which an individual becomes the object of special attention by observing specific characteristics or behaviours according to which, by extrapolating the information concerning him (*knowledge discovery in databases, data mining*), several profiles of attention or suspicion are created.

Profiling is one of the most used techniques, for example, to combat terrorism and implies, without judicial review, the placement of certain subjects, based on data collected without their knowledge in specific risk categories, precluding an opportunity to access some countries or to enjoy certain services. These cases of preventive and informal profiling have always been a useful part of the operational police practice¹⁰. But now technology increases the possibility of biomonitoring to the point of being able to constitute, if applied in a widespread and indiscriminate manner, an inversion in the burden of proof by which the presumption of innocence, the foundation of the protection of individual freedom and the rule of law, could become a form of presumption of guilt. In extreme cases, a person may be forced, without having committed any specific crime, to justify his overall behaviour to show that he is not a danger. But it is also possible to hypothesise possible discrimination in access to jobs and in many other spheres of economic and social life.

Therefore the dangers of profiling should be properly emphasized, prohibiting the crossing of data susceptible to stigmatization or exclusion and allowing use only in relevant cases, legally predetermined, with adequate

⁹ EC - Working Group for the Protection of Persons concerning the Processing of Personal Data, Opinion 3/2005 on the implementation of EC Regulation 2252/2004 of the Council (December 13, 2004), on standards for security features and biometrics in passports and travel documents issued by Member States - WP112 (Official Journal L 385, 29.12.2004, pp. 1-6), adopted September 30, 2005.

¹⁰ Strictly speaking, the origins of the investigative technique of profiling are traced back to the Fifties, when the New York police made use of psychiatry to put together heterogeneous clues designed to rebuild the possible profile of the person responsible for a series of attacks. But already in 1879 Alphonse Bertillon, a famous French police inspector, had proposed a system of anatomical measurements (including the length of arms and feet) to identify and record repeat offenders.

safeguards and control by means of organs of guaranteed impartiality. From this point of view, it would also be important to provide a right of access, tending to be unconditional, allowing each subject concerned to know what data have been collected on his behalf, by whom, for what purpose, since when and for how long.

It is to be borne in mind that the establishment of archives to permanently store some personal data of particular importance (e.g. civil or criminal records) has always been the sole responsibility of the State, strictly regulated and designed to ensure certainty in relations and public security. Today, the facility of computer storage processes multiply the technical possibilities, absolutely heterogeneous and non-codified, to build private databases. Public primacy in the establishing of identity remains tied to the duty to ensure safety, but this pre-eminence no longer corresponds to a monopoly over personal information, on the contrary, private databases (in the broadest sense of the word), now far exceed, in quantity and quality, public databases. There is also a constant mix of public and private sectors: the State takes information that tends to be private (e.g.: health, financial circumstances etc.), and the private sector takes information of public importance (e.g. identity that is required for travel, to complete commercial transactions, etc.).

All this, in some ways, makes it increasingly difficult for the citizen to verify and monitor compliance with protection rules (at times this control is purely administrative or contractual, but sometimes it is neither one nor the other). In other respects, the general use, public and private, of biometric technologies and their associated potential profiling as well as the extensive spread of archives, could make people insensitive to the risks related to protection of their privacy, creating a sense of helplessness and indifference in which it is easier for the progressive consolidation of a biomonitoring society characterized by a dangerous resignation to confusion between the physical person and the virtual person.

3.2 Essential bioethical profiles

3.2.1 The human body as password

In biometrics, the body becomes a real instrument of recognition and, therefore, to guarantee authentication new and specific measures are needed. In general terms, the physical or behavioral characteristic adopted for recognition and used at the time of the first registration in the system should be as similar as possible to those acquired at the time of the actual biometric transaction.

The technical obligation is realized, in practice, only in apparently simple actions. For example, it is a requirement, in biometric documents, that the facial expression assumed in the reference photographs and replicated at the time of the transaction should be as neutral as possible and therefore more easily reproduced. In this regard, there are already appropriate guidelines and explanatory tables, prepared by the organizations responsible for the standardization of data, to provide precise information on the facial expression to be assumed both during the stages of registration in the biometric system and that of authentication. In the light of emergent trends in technologically advanced countries, these instructions should also be extended to children, by

so doing they would be completely assimilated to the adult world. In addition, fingertips, whose exudate allows the collection of fingerprints, should not be damaged throughout life, for example by hand contact with corrosive acid. Similarly, if the biometric feature were the iris, in the case of cataract operations that would alter its morphology, the user who wants to safely preserve his 'biometricity' should re-register in the system due to the possible alteration of the morphological characteristics of the iris.

It is clear that the needs of recognition can have profound implications in the context of social life, by imposing new rules of conduct likely to take on deep bioethical implications. The idea is taking hold that, for reasons of security and certainty in relations, it is necessary to introduce a kind of duty for *permanence* and *maintenance* of the biometrics of the body that is unprecedented in cultural history and juridical experience (see section 4.4). The rules currently in force in the context of fundamental freedoms allow the individual adult and to some extent even minors to dispose at will of their appearance and not to worry particularly if their fingertips are altered or their face reshaped by plastic surgery. The alteration of the body is an atavistic manifestation of personal liberty on the basis of social, ethnic, religious or aesthetic trends or even just for fun. This applies both to non-permanent changes in appearance (cosmetic type changes, ornaments, etc.) and to permanent ones (tattoos, piercings, surgery, etc.).

In future, these habits may undergo a drastic reduction, even simply voluntarily, to avoid having to rebuild social identity whenever biometric credentials prove unreliable, as occurs with a worn or altered paper document. The way of appearing could therefore become the predominant way of being, the way in which each individual shapes their own unique image in relation to the deepest needs of their personality. Image, the symbol of personal identity, the personal instrument which each individual decides to proffer to the gaze of others and to communicate something of oneself to others, could turn into a pure constraint, the instrument by which the processes of identification are imposed.

It becomes obvious at this point, beyond the regulatory or coercive issues in general, that biometrics will however have profound psychosocial factors in the near future, including the possible feeling of uncertainty related to image and one's ability to be recognized by biometric systems.

3.2.2 Voluntary non-permanent changes

Voluntary non-permanent changes in appearance are generally the responsibility of biometrics based on facial recognition. In this category are placed all reversible changes ranging from cosmetics to the use of ornaments, up to the natural trichological change of the face.

Unfortunately, the effects of these changes as concerns the accuracy of face recognition are not completely known. What has been most studied is the problem posed by the use of glasses: for eyeglasses there would seem to be no particular difficulties as long as the lens does not cause a significant magnification of the periorbital area, the use of certain types of sunglasses can still be seriously harmful to the success of biometric transactions, even if some technologies, that reduce to zero the influence that they exert on the accuracy of biometric recognition, are in the advanced stages of testing.

3.2.3 Voluntary permanent changes

The increasing use of biometric technologies for investigative or judicial purposes is causing the growing problem of voluntary permanent alterations of one's biometric characteristics, both for aesthetic reasons and in order to deliberately avoid possible identification. To date, this phenomenon affects in particular the sector of biometric fingerprint recognition, as fingerprints can be intentionally damaged to the point of rendering a person totally unidentifiable. In general, this problem must also be assessed in order to prevent abuses and crimes could be perpetrated also on third parties (sometimes even on children).

3.2.4 The duty of conservation of biometric features

As occurs in current practice for traditional paper documents, if deteriorated, they may be rejected as an identification document, in the same way, in a future of ever more extensive biometric transactions, the damaging of one's biometric characteristics, such as atypically worn fingertips with the consequent difficulty in the issue of fingerprints, could have important effects in terms of recognition. In some cases, similar to what happens in the case of deteriorated documents a damaged biometric feature could lead to a refusal of the transaction by those responsible for control or by the system itself.

At this point, the limits of biometric technologies compared to traditional methods of recognition, should be rightly pointed out. While it is possible to reissue of an identity card similar to the deteriorated one and formally correct, in the case of biometric features, the physical element, once altered, may never be suitable again for recognition. This would create a sort of *biometric inability* for that physical feature.

3.2.5 Right to anonymity

Since biometrics works, by definition, through the attribution of identity or its verification, interference with the social systems of security is certainly likely. Preservation of the personal sphere as a fundamental intimate element implies the existence of a right to anonymity, or at least to exclusion of large spheres from the control of others. Confidentiality can not, however, justify an absolute right of non-interference each time someone is exposed to the public or adopts behavior that involves relations with other individuals. In other words, there is no absolute right to anonymity, which however, is guaranteed in many different circumstances. The cases in which it is desirable is the subject of discussion and moreover biometric technologies could reduce that freedom.

A clear example of the sensitivity of the subject can be supplied by the heated exchange of views in countries that are planning the construction of identity cards based on biometric identifiers. The process necessarily involves the development of national identity registers and some observers, as well as parts of public opinion see this as a serious attack on personal freedom and anonymity. The risk is further increased due to the potential application of the techniques of profiling that is spreading increasingly.

3.2.6 Discrimination of certain sections of the population

An important aspect of biometrics with clear ethical implications is given by the possible discrimination of certain groups of users. Of course, as well as the handicapped, for which the use of biometric technology is however in general terms, more complex and requires special measures, there is frequently open talk about *biometric disability* and namely about the difficulty or impossibility to use biometric technologies, encountered for certain categories of users.

It is known that, as with other phenomena related to human nature, including matters relating to biometric technologies, there is a window of time over which system performance is optimal. However, if biometric applications, as in the estimates of experts, become commonplace, they will affect people of all ages and it is already known, for example, that people from ages higher or lower than the "optimal" may experience some difficulties in using these technologies.

For example, if we refer to fingerprint recognition, biometric technology par excellence, the gradual drying of the skin combined with a thinning of the papillary ridges, phenomena related to age, causes an important loss of definition in the acquisition of fingerprints, to the point that some biometric programs for immigration fix a maximum age limit for the issue of fingerprints¹¹. Similarly, there are no clear indications on the temporal stability of the vascular characteristics underlying many new biometric technologies.

Any automatic equalization of the human body to a password does not consider with due attention the temporal transience of individual physical elements used for recognition. At present, there are no biometric technologies able to compensate, for biometric authentication purposes, for the inevitable changes caused by increasing age, changes that at times even make some of these technologies unusable (making appropriate the imposition of strict age limits for use). The analysis of the blood supply to some parts of the body, which is considered suitable for application without excessive age limits, is probably still too recent to be able to understand its real potential.

A futuristic alternative to such strict limits might be the use of variable thresholds of biometric systems according to the age of the user (in possession of an electronic card containing personal data). This approach, despite causing unavoidable increases in costs of design and operation of a biometric system, could allow the overcoming of rigid discrimination based on age, making older people feel more included in technological processes. Being excluded *tout-court*, could in fact increase their feeling that increasing age corresponds to a tragic loss of potential, even in terms of the use of innovative technologies.

The same applies to children¹². For them, the use of biometrics raises a number of technical as well as ethical problems, and in particular for the fact that in this category of users body parts usable for the acquisition of biometric data are not yet fully formed or are still undergoing rapid development. One of

¹¹ A similar situation, the inherent limitation of the collection of fingerprints, also affects children, whose fingerprints are still undergoing fast and profound change. This could lead to substantial unreliability of the techniques and above all the need to continually update the template, with extremely high frequency.

¹² In this case, it applies to a segment of the population that, in general terms, ranges from the age of 2 to 14-15.

the most delicate aspects is also represented by the almost total lack of specific studies.

While there is no denying the strong ethical value underlying biometric technologies as related to the fight against human trafficking, especially children, strongly influenced and limited by the use of these technologies, it is equally true that the use of biometrics for children should be defined in a context of strong caution for the possible psychological effects potentially related to the use of technologies that, at least at present, are perceived by the public as related to investigative and judicial aspects.

In fact, this characterization refers primarily to the use of fingerprints that over the years have actually proven to be of valuable support in public order operations. It is also true, however, that there are other biometric technologies which, having been developed in recent years, are characterized by less immediate psychological connections and perhaps should be preferred in applications aimed at children, for example access to school buildings, so as not to make them associate the biometric process to other procedures employed with a certain severity in different contexts.

Biometric facial recognition seems, at first, the most appropriate technology to use in the world of children even if, due to significant somatic changes even of the face, the so-called *currency* that represents the temporal parameter by which facial recognition has a good chance of success, is low and therefore measures are required, such as repeated enrollment in the biometric system.

Lastly, apart from the forms of exclusion linked to these new manifestations of *biometric disability* or inappropriate use of certain technologies for certain sections of the population; the use of instruments for detection, including biometric technologies, when applied only to a part of the population is to be condemned, if it jeopardizes the constitutional principle of equality.

4. Long-term scenarios

Producing forecasts on a larger and longer term scale, some experts argue that biometric technologies will represent only the tip of the iceberg as regards the thorough analysis to which users will be subjected. The information derived from biometric observation is in fact definitely higher in number and quality than those required for the single transaction with these technologies.

For example, as highlighted in section 3.2, through the single biometric recognition of certain physical features (e.g. face, retina or iris) a variety of information can be derived relating to the clinical picture of the user, and especially as to his psycho-emotional state, with all the potential risks of possible dissemination or improper use. Similarly, growing video surveillance in public places and simultaneous (hidden) biometric recognition could trace all movements of a person, as far as identifying their preferences in terms of purchases or the people they frequent.

Certainly, today's technological level, which is currently limited, and the irrelevancy of acquiring and retaining such a large quantity of information (an excess of facts are produced which can not be managed for any purpose) lead to the belief that there is no real danger of shady scenarios. However, it seems appropriate not only to take note of the indisputable merits related to individual

and collective security and more generally the quality of life of individuals. Instead, there should be an examination of the negative consequences of this pervasive and stubborn accumulation of data, which could affect the fundamental liberties and each individual's relationship with others and with his body, setting some limits in the use of biometric technologies that make their use more appropriate ethically and socially.

4.1 Preference for the use of technologies based on biometric features that leave no traces and for the exclusion of centralized repositories

As biometric technologies spread, it is easier to make a classification both, as we have seen, as regards the context of application that is most appropriate technically and in terms of possible social risks for users.

An interesting classification has been proposed by the *Commission Nationale de l'Informatique et des Libertés* (CNIL) in France, regarding biometric technologies that leave or do not leave traces. The CNIL refers to 'material' tracks, or the fact that the fingerprints, for example, are left everywhere on the objects we touch and therefore could be captured at a later time by anyone and, possibly used fraudulently. The spread of biometrics makes this a realistic possibility on a larger scale.

In principle, one can say that the risk, that biometric data obtained from physical traces left by an individual without his knowledge (e.g.: fingerprints) may be used for improper purposes, is potentially less if the data, instead of being stored in centralized repositories, remains with the same person through the use of electronic cards (Verification of Identity) without being accessible to third parties¹³.

A centralized repository of biometric data also increases the risk that such data be used to connect to other aggregates of personal data creating collectively a profiling of the subjects concerned. Biometrics could in this way act as a connecting element between heterogeneous information producing consistent information on the private lives of individuals and their habits in a variety of different fields. In this sense, different databases will be interoperable, while on the one hand it generates efficient systems and it can be an added value of biometrics as an enabling technology, on the other hand, it gives top interconnection of data with all the possible associated hazards¹⁴.

It is therefore clear that the use of technologies based on biometric features that leave no tracks, and that are based on the preference for systems with low impact archiving, and nonetheless, archives that are not interoperable, would solve some of the ethical and juridical issues related to biometrics, mitigating the potential mistrust of the users.

4.2 The right to oblivion

Memory is a key element of individual identity and social relations. It is difficult to imagine any internal development and cultural progress without the

¹³ EC - Working Group for the Protection of Persons concerning the Processing of Personal Data, Working document on biometrics, 12168/02/IT - WP 80, adopted on 1 August 2003.

¹⁴ Idem.

conservation and organization of traces of the past which may take many forms (memory, history, opinion, prejudice, etc.). Oblivion is just as important to make a selection within this set of elements, avoiding any unnecessary or harmful accumulation. To ensure social stability and protect the fundamental rights and freedoms of individuals, juridical experience has had to develop artificial forms of oblivion (despite their diversity: removal from criminal records, prescription, amnesty, pardon, etc.), where morality entrusts to forgiveness the extreme inner effort to overcome the past. From this point of view, biometrics does not present anything new: it merely offers a more intense, diligent and capillary collection of the amount of information. However, in order to be, at the same time, more systematic and fragmentary, more diligent and sporadic, biometric detection accentuates the possibility of interference in the lives of individuals. If economic developments and the right security requirements undermine any claim to guarantee an absolute right to anonymity, it becomes crucial to develop new and more complex forms of the right to oblivion. This is what currently happens with the biological material that is anonymized (that is, linked to symbols or numeric codes to prevent being traced back, without authorization, to the identity of the person to whom they belong). By so doing, this ensures the confidentiality of all the information of the original referent, without preventing, in exceptional cases and under certain conditions, that identity can be traced (provided that the person has not requested irreversible anonymity). The same model should be followed for biometric detection, so to provide reliable and transparent processes of erasure or anonymity, and strongly reaffirm both the principle of exceptionality of the accumulation and crossing of information, particularly when information is acquired through non-cooperative and hidden instruments, and banishing vigorously any attempt to *function creep*.

Particular attention should be paid by individual legislators and international organizations, to make the right to oblivion effective, not only by providing fast and simple forms of its exercise, but by clearly placing the responsibility on whoever recorded the data, to obligatorily prove the necessity, proportionality and relevance of their collection. Memory, when it is entrusted to the schematics of *ubiquitous and autonomic computing*, can become a subtle and irreversible form of discrimination, being condemned to the impossibility of escaping the traces of one's past. For this reason, oblivion can not continue to be regarded as an exception, an individual or social concession linked to distressing moral choices or to particular situations. It must become an aspect of the fundamental right to personal identity, the right not to be filed, classified, and possibly irreversibly marginalized on the basis of information gathered without your knowledge through non-transparent criteria and for largely unknown purposes. The growth, in terms of efficiency and security, of biometric acquisitions should therefore be accompanied by a proportional increase in the possibilities of protection and hopefully in public awareness. If anonymity can not be expected, it is essential that at least the conditions for oblivion are guaranteed.

5. Summary and Recommendations

The widespread introduction of biometrics in civil life could in principle interfere with that degree of confidentiality that is currently recognized to the

person from the ethical and juridical tradition. Therefore, it is necessary that any such initiative should be adequately justified in terms of necessity and proportionality, accepted by public opinion and governed by the State, with proper assessment of the relationship between benefits and risks in the different sectors of peoples' public and private lives.

The NBC believes that the use of biometric systems for identification is extremely important to facilitate access and enjoyment of services, human relations, management of health, trade and financial transactions, and in general for purposes of facilitation. In particular, biometrics is crucial to improve safety, which in turn is a fundamental condition for the exercise of freedom and the achievement of individual personality. In addition to being safer and easier to use biometric systems could themselves be classified as technologies capable of increasing the spheres of confidentiality¹⁵, for example by avoiding having to provide any sensitive data that are now indispensable in the process of identification (eg.: date of birth, sex, nationality, marital status, home address, etc.).

These undeniable advantages do not prevent the indiscriminate use of biometrics, on the grounds that they create the material conditions that can enable various subjects to acquire, permanently connect and use, often in a covert manner and for a variety of purposes, a plurality of physical and behavioral data that could however determine consistent risks of discrimination, stigmatization and exclusion.

One form of such discrimination would occur for example each time these resources are used only against a part of the population in order to emphasize social control, but also to discourage inclusion in social life or to emphasize a "difference". Then there is the possibility of a particularly frustrating discrimination for individuals on the basis of system errors which can not be easily corrected, given the complexity and number of databases as well as the intersections between them. Stigma may be generated through the process of *profiling* creating, *a priori*, "suspect" profiles based on physical or behavioral characteristics by which certain persons may be prevented access to certain places or enjoyment of certain services. The phenomenon may be both public (e.g.: the fight against terrorism and organized crime) and private (e.g. the refusal of certain medical services to a certain group of subjects), and presents elements of special concern if it occurs in a hidden manner, perhaps linked to the use of distorted information acquired in excess of that go well beyond the purpose of immediate identification (*function-creep*, cf. section 3.1). Cases of exclusion could relate to certain categories of users (the elderly, children, and people with disabilities) that would become genuine *biometric disabled*, excluded from the use of certain services or access to particular places, or however forced to deal with even very expensive difficulties and obstacles.

Moreover, discrimination, stigmatization and seclusion would increase the risk that in psychological terms the subject becomes increasingly conscious of the body as something foreign, hostile, an enemy that belongs more to society, through the multiplicity of identification processes and the infinity of recorded and used tracks, than to himself and to the free explication of personality. All this would be even clearer and deeper should there be a duty for *permanence* of one's biometric data and *maintenance* regarding each of them.

¹⁵ PET (*Privacy Enhancing Technologies*).

In the light of possible inappropriate uses and potential risks of biometric technologies, the NBC recommends:

1. for the protection of the person:
 - a) that the introduction of biometric systems takes place continuously on the basis of the principles of necessity and proportionality;
 - b) that the application of prior informed consent should be guaranteed as far as possible to data collection and use, giving full information to its purpose;
 - c) that the use of technologies that involve a limited use of centralized and interoperable repositories should be encouraged;
 - d) that there should be recognition of the right to access of the person concerned to the biometric database regarding him, to know what data have been collected, by whom and for what purpose, since when and for how long, and with what other data this has been associated;
 - e) that there should be recognition of the right to oblivion considered an aspect of fundamental human rights, providing as far as possible reliable and transparent processes of cancellation or anonymity of biometric data, furthering in any case the idea of the exceptional accumulation of data and intersection of information, particularly when acquired through non-cooperative and hidden instruments.

2. for the organization and regulation of biometric applications:
 - f) that public and private legal entities or the authorities responsible for the collection of biometric data, and their purpose should be clearly identifiable;
 - g) that there should be established, in addition to the Authority for the protection of privacy and in close cooperation with it, a third body that controls whoever acquires biometric data, in what way and for what purpose, and how they are managed; or, alternatively, the NBC recommends the strengthening of the functions and responsibilities of the Authority for the protection of privacy, in order to address the combination of ethical and juridical profiles of biometrics;
 - h) that a framework measure should be developed and adopted, as was done for video surveillance, in order to regulate the use of biometric technologies and their management.

Lastly, the NBC hopes that intervention will be in force in all European and International countries to adopt domestic legislation prohibiting all forms of discriminatory application, preventing any use of biometrics that is unjustified or for purposes different to those proposed (function creep), incorporating the principles of *biometric disability*, and specifically the inability or difficulty to use biometric technologies that are sometimes found in certain categories of users.