



**Commission nationale
de l'informatique et des
libertés**
21, rue Saint-Guillaume
75340 PARIS CEDEX 07

- 22nd ANNUAL REPORT FOR 2001 -

EXTRACTS OF CHAPTER 3 « CURRENT DEBATES »:

- A CENTURY OF BIOMETRICS

A CENTURY OF BIOMETRICS

Biometrics is usually quoted as one of the new technologies which will see sizeable development in the coming years. Biometric systems can be defined as applications allowing automatic identification or a person's eligibility for having certain rights or services recognized (particularly access) based on the recognition of physical specificities (fingerprints, the iris of the eye, the outline of the hand, etc.), of traces (DNA, blood, odours), or behavioural elements (signature, gait).

The Commission has in the past consecrated numerous developments to certain biometric techniques, whether it concerns identification by DNA (see 20th annual report for 1999, p. 29) or by fingerprinting (see 21st annual report for 2000, p. 101). But biometric elements are diversifying, the biometrics market is expanding and certain biometric recognition or identification techniques are raising new ethical problems, such as for example, face recognition. These observations have led the Commission to undertake a study of all these technologies which are more and more frequently used, particularly due to a considerable decrease of their cost.

A. Some technical observations

1 – COMMON CHARACTERISTICS OF ELEMENTS OF BIOMETRICS

Universality: the biometric element should exist in all people. This formula appears obvious; it is not. For example, retinal biometrics is compatible with the use of contact lenses but it excludes blind people as well as those who have a declining cataract; the process of recognition by the iris is less efficient when contact lenses are worn, even if a French supplier of this technology assures us that the system he proposes works with sunglasses! Recognition by the outline of the hand presents certain problems for children (hands too small), and the CNIL was consulted on a system of access control using the outline of the hand for the reason that the fingerprints of the concerned population, cleaning personnel in a public establishment, had been damaged by detergent products.

Uniqueness: the biometric element must be distinctive to each person. In this respect, not all biometric elements are equivalent and the rate of distinguishing one person from another is very different, according to the type of biometrics used. The most distinctive biometric element is DNA, but also the retina and, of course, the fingerprint. But recognition by the iris, less discriminating than retinal recognition, would be more so than the fingerprint. Face recognition is considered more discriminating than the outline of the hand, the voice or the handwritten signature. In any event, the distinction is very clear. The probability that one person's iris resembles that of another person is 1 in 10^{78} , when the size of the human population is estimated to be 6 in 10^9 .

Permanence: the property of the biometric element must remain permanent over time for each person. One might imagine that such a characteristic would immediately exclude certain biometric elements, such as the outline of the hand (that grows each year), the voice that changes, or the face that ages. However, technological progress is so considerable that it allows us to anticipate certain evolutions of the biometric element. Face recognition processes are, thus, designed to identify faces in $\frac{3}{4}$, other technologies include warning systems when it is necessary to make a new recording of the biometric comparison element, and a cold does not hinder recognition in the procedures of voice recognition which are based more on the physiological characteristics of the vocal apparatus (i.e. the whole formed by the lungs, the vocal cords, the trachea, the throat, the mouth and the lips) than on the sound of the voice.

Accessibility and ability to be quantified: is the last characteristic of the biometric element, which must be collectable and measurable, in order to be compared.

The collection is carried out during a phase called “enrolment” which the commercial people like to call “the recording ceremony”. The collection of primary data (image of the fingerprint, characteristics of the iris or of the retina, recording of the voice) is carried out using a sensor specific to each type of biometrics.

The measure is based on what the technicians in the matter call the “template”, which is a structured reduction of a biometric image. It is the template, presented in the form of a series of digits, which will be stored and not the biometric element itself. In this manner, from a size of images of a million or more octets, the calculated template occupies at most a few thousand octets. The template is original and specific to each manufacturer or editor of biometrics technologies, and its exact structuring is not meant to be made public.

The professionals concerned point out that the expression “fingerprint file” is incorrect, as the file contains only the template of the print and not the image of our finger. This is obviously for the convenience of language: we usually say “fingerprint file” just as we say “genetic print file”, the expression given by the law to name the file of DNA templates of individuals convicted of certain crimes.

Out of the same concern for reassuring public opinion, considering the police connotation of these technologies, their designers point out that it is impossible to either store, reconstitute, or recreate from the template the image of, for example a finger, if the technology is that of the fingerprint. That is true but rather unimportant, insofar as, in applying the algorithm used by the designer of the database to the trace of a finger found on a table or a glass, one can easily find out if the person is on file in the database and, if so, who he is, by comparing the two templates.

2 – THE COMMON CHARACTERISTICS OF BIOMETRIC RECOGNITION SYSTEMS

The performance of the system. It is measurable in terms of errors and speed of identification.

Two error rates are used to define the potential of a biometrics technique and the precision of a practical biometrics system. The first rate is that of statistical frequency of a mistaken reject, i.e., the non-recognition of someone who should have been recognized. This is called FRR, False Reject Rate. The second rate defines the statistical frequency of an accepted imposture; i.e., the system has mistakenly recognized an individual who should not have been accepted. That is FAR, False Access Rate. The optimum of the combination of these two rates at their lowest (the EER) is the element used to define the performance of a biometrics technique. These rates, which are calculated theoretically under experimental conditions, obviously merit a closer assessment when the system is really implemented. One may, thus, go from a commercially announced FAR of 0,1% to a much higher FAR in practice.

Another adjustment of these rates may be defined by the user of the system who may choose' to reduce the risk of false reject by preferring to admit an error or, just the opposite, reduce the risk of a false access when, for example, the security of an installation is in question.

A concern for security or mediocre performances of a technology can sometimes lead the user of the biometrics system to combine it with other identification or authentication technologies. Certain arrangements could thus, for example, cumulate face recognition and voiceprints. On a computer keyboard one could type a password, present one's fingerprints, and introduce a microchip card. We then find a triple rate of authentication, as we know (the password), as we own (the card), as we are (the biometrics element). This association of a biometrics technology with other more current recognition processes is called multi-modal biometrics. An example of multi-modal use can be found in Israel where they have installed identity controls by face recognition and outline of the hand, memorized on a microchip card, at 42 crossing points for Palestinian day labourers.

User tolerance. This is an extremely important factor which is subject to qualitative studies. As an example, retinal control, based on the characteristics of the vascular network which forms an image accessible through the pupil by the use of a sophisticated apparatus, is considered particularly uncomfortable. The user, in fact, has to press his eye against an eyepiece through which passes an infrared ray, naturally, of a totally inoffensive intensity. But the recording becomes impossible if the eye is removed more than three centimetres from the reader. This technology is, therefore, used in practice only for extremely high security access. It is today used for certain FBI personnel and American, Swiss, Spanish, and Swedish military personnel. On the other hand, tolerance of Iris recognition is much higher, as the distance between the eye and the sensor is of about 60 cm. The manufacturers promoting this technology point out that it is adapted to large-scale recognition, for example, to control airline passengers. On this subject, a study is currently being carried out by BioTrust in Germany to evaluate the tolerance of 8 different technologies.

Robustness. This is the quality characterising resistance to falsification or imposture. This question, naturally, preoccupies the manufacturers considerably. Certain fingerprint recognition processes, thus, verify that the finger presented is alive (by checking blood circulation and the heat given off).

Finally, the last quality is that of the system's **ability to interface** with other computer systems.

B. A special case: the rapid growth of face recognition technologies

1 – A BRIEF HISTORY FULL OF PROMISE

Most of the scientific articles agree on 1973 as the year when the first scientific publication treating the theme of face recognition appeared, with the article by the Japanese, T. Kanada, "Picture processing by computer complex and recognition of human faces". But, the number of scientific publications on the subject began to grow only at the end of the '80s.

1991 was a turning point in matters of theoretical research, with the the publication of the article "Eigenfaces for recognition", by Pentland and Turk of MIT (Massachusetts Institute of Technology). The article described a revolutionary algorithm, the "eigenfaces", which had the merit of taking the theme of face recognition out of the "academic" framework, to which it had been confined until then, and of allowing them to move on to a more "operational" phase. Thanks to the means of the MIT, Pentland and Turk could, furthermore, support their assertions by real and significant experimental data.

The move towards commercial products received a decisive impetus as from the years 1994-96 due to the implementation of the FERET (Face Recognition Technology) programme organised by the American Department of Defense (DoD). The name of the department of the Ministry charged with piloting the project (“counterdrug”) speaks volumes on the objectives of this programme: “develop automatic recognition capacities in order to help the work of the security and espionage, etc. department personnel”.

At the end of the evaluation tests in 1996, all the actors of the world of face recognition, research laboratories and manufacturers, disposed of a reference database. In fact, until then, apart from the MIT database, each laboratory had its own base of images, at most comprising 50 individuals. The FERET database contains 14 126 images for a total of 1199 individuals. A person may have been photographed several times, either the same day or at an interval of one to two years, which is a precious element towards evaluating the influence on face recognition algorithms of a change in the appearance of individuals due to age, hairstyle, lighting, posture, etc.

Completely different products were also compared on objective databases, and the insufficiencies or the limits of each algorithm were shown.

Since the end of the FERET project in 1996 the big change has been the appearance of commercial products on the market. The high competitiveness of the market has made a large number of face recognition algorithms, or of variants, appear, most of which were not even present during the FERET evaluation tests, and at more and more competitive prices. Today, according to the American Department of Defense Web-site, “there are dozens of face recognition systems potentially capable of satisfying the performance constraints of numerous applications”.

The American Department of Defense then decided to launch the FRVT 2000 (Facial Recognition Vendor Test 2000) programme whose objective was to evaluate the performance of commercial products.

Thus, the face recognition techniques are not only theoretically viable (this was the result of the first FERET evaluation test in 1994), but a level of industrial maturity now seems to have been reached.

2 – AN EXAMPLE OF MASSIVE IMPLEMENTATION

On 14 October 1998 the London Borough of Newham (a popular neighbourhood to the East of Greater London) installed a system designed to reduce the number of crimes and offences by 10% in 6 months, using a face recognition software called Mandrake. The system alerted the video camera operators when there was an 80% concordance between the previously digitised image of a delinquent and that captured by the cameras. 100 photos of offenders from the files of two local police stations were digitised. The Mandrake face recognition software was installed on micro-computers for analysing the images captured by 140 video cameras.

This project was criticized by the Data Protection Registrar (the opposite number of the CNIL in the UK) who was concerned about threats to privacy, but the municipal Council replied, that the system contained no personal data, but only photographs and police reference numbers! It was, however, strongly contested by numerous Human Rights associations.

Eighteen months after the system was implemented, the municipality congratulated itself on a decrease in criminality, and the British Prime Minister went there accompanied by the Home Secretary.

3 – SOME OTHER APPLICATIONS

The air transport industry is very interested in face recognition technologies, insofar as, if installed at the passport control point, they would allow a comparison between the passport photo and a database of wanted persons.

The control of certain crowd-attracting “large events” will, no doubt, become a favourite domain for the use of face recognition. In this manner, during the “Super Bowl” (the big final in American football) which took place in Tampa, Florida, in January 2001, the local authorities used video-surveillance associated with face recognition to watch the stadium in order to spot any possible wanted criminals.

Other recent uses of face recognition can be quoted. During the presidential election in Uganda in March 2001, each of the ten million voters received a microchip voting card containing the template of their faces. During the vote, the voter's face was compared by a software in real time to that recorded on the card presented. Reduction of electoral fraud (multiple votes by one single person) was apparently considerable. Wishing to hunt down fraud in means of payment, a large distribution chain in South Africa issued a microchip card to volunteer clients (1600 clients at the end of 2001) showing their faces in template form. When the client goes through the tills for payment, his face is compared by software to that memorized on the card. As the traffic in false papers is rather widespread in that country, having recourse to biometrics has seduced numerous companies. To control the 40 000 Palestinian day labourers at the 42 border crossing points with Israel, face recognition is used combined with the outline of the hand.

In these examples, the recourse to face recognition is justified by its promoters as being of little constraint to the user who accepts it; furthermore, the rate of recognition may be very high, the photograph of the faces having been previously recorded in a standardized framework.

The tragic events in New York on 11 September 2001 should be a turning point in large scale use of face recognition in the United States, both in the form of “video-surveillance”, after the Newham model, of public places, particularly airports, and for the control of identity papers at border crossings.

4 – A LITTLE ABOUT TECHNOLOGY

A robust recognition process should be able to recognize identities despite variations in the appearance of a face during a scene. The face, which is in three dimensions, is not only submitted to lighting of very variable contrast and luminosity, but can, moreover, appear against a background which itself comprises other faces. This three-dimensional form may give rise to important variations, when it appears against a two-dimensional surface, as is the case in an image.

The system of recognition must also be capable of tolerating variations in the face itself. A face is not rigid, it may undergo a large variety of changes due to an expression (joy, sadness, etc.), to age, to the hair, to the use of cosmetic products, etc.

Face recognition systems may be classified roughly in two major categories: on the one hand, the methods based on the recognition of the characteristics of a human face, and on the other hand, the so-called global methods.

The methods based on the characteristics of the face seek and analyse the characteristic elements of a face, such as the eyes, the mouth, the nose, the cheeks, etc. After processing each of these elements, all the obtained results are combined to proceed to recognition of the face. One can, for example, define the template of the face from these elements, particularly by calculating the distances separating them (distance between the two eyes, between the two cheeks, etc.), their respective proportions, like in anthropometry. This category of methods is resistant to variations in position of the face in the image.

The so-called global methods process the image as a whole, without trying to isolate specifically each of these “regions”. The global methods use, for example, statistical analysis and spectral analysis techniques, etc. The strength of the global methods is that they use all the characteristics of the face, without giving preferential treatment to certain “regions”. Naturally, if we take the example of a method based on statistical analysis, the “weight” of an eye, of the nose or of the mouth on the final result should be higher than that of a freckle on the cheek, but it is the statistical analysis of the image pixels which will discover it quite “naturally”. In general, the global methods give good rates of recognition, but require that the face be presented in a simple frame: presented almost full-face, regular lighting, simple background. The performances degrade rapidly when there are changes in the positioning of the face, when the lighting varies abruptly, or the background is too intricate.

In the most efficient products, the quality of recognition is relatively insensitive to changes in face expression, including blinking the eyes, a sulky expression, or smiling. The growth of beards or moustaches is compensated by collecting other, sufficiently diffuse and reliable, elements of the face. The hairstyle has no importance as the hair is not one of the elements used in the calculations.

Where it concerns positioning, an orientation of less than 10-15° deviation from the frontal position presents no degradation in performance. Between 15 and 35° the performance decreases. Beyond 35° recognition is not good, but the faces can still be compared with other faces turned at the same angle, provided the eyes remain clearly visible.

Certain products emphasize the fact that the performances are not reduced when the child grows from adolescence to adulthood.

To detect that the person does not present a photograph of a face instead of the face itself to the camera, the presence of outline characteristics that one may find in a photograph are looked for, such as, for example the rectangular frame. The user may also be invited to smile or to blink his eyes. The test of a “live” face lasts on average 2 to 3 seconds.

The main causes for recognition error are: a too bright light reflecting off glasses making eye detection impossible; hair that is too long darkening the central part of the face; insufficient lighting that overexposes (blackens) the face and reduces contrast; a too low image resolution (insufficiency of pixels).

The principle of discovery and tracking by video camera is particularly formidable: it consists, firstly, in recognizing an individual's face, then in following him, based on his outline characteristics and the texture of his flesh. The tracking can continue despite the person turning his head, even completely.

5 – A FUTURE UNDER SURVEILLANCE?

Face recognition technology is presented by the MIT (Massachusetts Institute of Technology) as one of the ten most promising technologies for the coming ten years.

In the eyes of the French “data protection law”, if the technique should develop and its results become more refined, two serious risks could be feared.

The first would be that of feeding the comparison database, by considerably increasing the number of photographs of the people to be looked for or to be watched. Originally limited to individuals officially wanted by the public authorities, in accordance with, for example, a warrant for arrest, could there not be a risk that one would look for simple suspects, and then for people not suspected of having committed a crime, but who, previously known to police services, could be put under permanent surveillance, in order to control their movements and prevent criminal behaviour?

The second risk would be that of an increase in the number of video-surveillance cameras installed in public places or places open to the public, briefly, a widening of the watched perimeters. In this hypothesis it would, moreover, not be necessary to store the captured images for long, insofar as the objective would be less to carry out general surveillance of everyone than to locate the places where the wanted persons could be.

Added together, these two risks indicate the temptations. It is appropriate at this stage to note that when a video-surveillance system is interfaced with a face recognition software, the law of 6 January 1978 is applicable in its totality, and the measure can only be implemented by an administration or a legal entity subject to public law after a favourable decision by the CNIL. Such a control is not applicable to the private sector, but in its current state, the project of adaptation of the European Directive submits all processing of personal data, including biometric data, to a system of authorisation. Such prior control by an independent authority is likely to prevent the risk of excessive proliferation of this technology, which will no doubt bring security, but which, in all respects, is a risk to our liberties.

C. The pertinence of legal means of personal data protection in seeking a fair balance

The technological progress and the diversity of use of biometric recognition or identification techniques, particularly encouraged by a decrease in cost, undoubtedly constitute a powerful factor of development and of making biometric controls relatively commonplace. The industrialists in the sector are at the same time making an effort to ensure a renewed interest in these technologies as far removed as possible from their police or security origins, by pointing out the variety of possible uses which have no connection with the police or wanted persons.

These efforts, designed to encourage public opinion towards a greater social tolerance of such technologies, are far from vain and each use of biometrics technology for other than police purposes is pointed out as an illustration of these new tendencies, even if it remains striking to note that the biggest applications, in any case mass applications, are carried out mostly in the Southern hemisphere, in developing countries or those that are particularly concerned about their internal security (Uganda, Israel, Mexico, the Philippines, and South Africa are very frequently quoted in this respect).

This observation, like the earlier developments on face recognition, should not give the feeling that the personal data protection authorities maintain particular mistrust of these technological developments. It is more their use and the opinion that a society has of itself that should be questioned. In this respect one cannot fail to note the great relevance of legal means of data protection in seeking a fair balance.

1 – THE PRINCIPLES OF PERSONAL DATA PROTECTION APPLIED TO BIOMETRICS TECHNOLOGIES

By nature, an element of biometric identification or its digital translation in the form of a template constitute data of a personal nature entering the field of application of data protection laws, like other personal data (a name, an address, a telephone number, etc.). The purpose of these techniques is, in fact, basically to recognize an individual, to identify him, to authenticate him, to find him.

In this respect, when the processing of biometric data implies storing the templates, a database is constituted which then comes under all the measures of the data protection laws, the first of which are the cardinal principle of purpose and the principle which is its corollary, implicit in our legislations, the principle of proportionality.

Principle of purpose and the database

In reality, the risk that a database of templates could be diverted from its purpose by those who created or implemented it is generally very low. As the professionals concerned like to stress, a template base implemented for the purposes of access control or authentication presents very little interest: one cannot, from the template, reconstitute the image of the biometric element used; a biometric element is objective and not very meaningful, less so in any case than other basic information, such as someone's taste, his level of debt, or his nationality.

The case of centralised databases for police or legal purposes is, obviously, different, because simply to appear in one of these gives information. A name associated with a DNA template in the national genetic print file for criminal purposes evidently means that the person has been convicted of a serious crime or is currently wanted as the presumed author of a crime or a sexual offence. Similarly, to appear in the national police fingerprint file means that the person has been implicated in a legal procedure. These examples alone show the extent of the fundamental principle of purpose.

But the risk of the use of biometrics databases for purposes other than those having justified their creation is a major one when the biometric element is one of those that “leave traces”. This is the case of DNA (a hair, saliva on a cigarette end, etc.), of the fingerprint that one leaves behind in all circumstances of life, as well as of the faces that can be captured by the video-surveillance cameras, still more numerous in both public and private places. A society encouraging the development of, for example, fingerprint databases would offer considerable and new means – at least “possible” - of police investigations, without such an objective having initially been sought. Not because the databases would have been constituted for police purposes, but because such, apparently insignificant, databases could be used by the police as an element of comparison and research in the framework of their investigations.

On this point, system designers point out that such a possibility is difficult to imagine, insofar as each industrialist uses his own specific template and the print template databases can be encrypted. But such precautions do not remove all risks: the police authorities, in fact, have the right to demand the designer of the technology to communicate the software characteristics of the template used, or the keys to decrypting the database. Furthermore, the fact that each database is supposed to be specific and to concern only a number of people too limited to be of any use in large scale police investigations may not be convincing, as several manufacturers in the sector use the commercial argument, that the biometrics databases they install are inter-operational, which may make us fear that the technical elements presented as guarantees are only very provisional and do not resist temptation.

Everything is, therefore, a case of measure and proportionality.

Databases of biometric elements which obviously leave no trace do not raise problems of this nature: a database for recognition of the voice, the template of the iris, the retina, or the outline of the hand can in no case be used for purposes other than recognizing and authenticating the person presented to the sensor.

Furthermore, the security measures surrounding the databases can, in certain cases, bring adapted responses to seeking this balance. During the 18th international conference of data protection authorities, which took place in Ottawa in September 1996, an American consultant, thus, presented a solution for preventing any possible police use of a database of fingerprints created for other purposes, so important is this question in a society of liberties. It was therefore recommended that the template of the fingerprint should be used to encrypt the element contained in the database: in this manner, each template of a fingerprint could only be decrypted in the presence of the person to whom the biometric information belongs. By placing the finger on a sensor, the characteristics of the fingerprint would produce a template, which being the key to decryption, could only refer to a single print whose template had been encrypted according to the same means during its recording, i.e., his own.

This original, but still prospective, solution would guarantee in absolute terms that a database constituted for purposes of access control could not be used for law enforcement purposes.

Using biometrics technologies without any social risk

The above observations lead us to stress that biometrics technologies have a considerable field of possible use devoid of any social risk, in any event to individual or public liberties or to the respect for privacy: such is the case, when the biometric recognition template is not stored in a centralised database, but remains with the person, inaccessible to any third party.

The possible applications are numerous: the inclusion of a voice recognition measure on a mobile telephone to prevent it being used by a third party, the use of fingerprints for the same purposes to ensure that only the user can have access to a micro computer, the inclusion of the fingerprint template in the microchip of a bank card allowing us to ensure, by comparison of a finger presented in the reader of the cash dispenser and the print included in the microchip, that the user of the card is really its owner. All these applications are subject to numerous feasibility studies by the professionals concerned, without such uses, at any moment, raising difficulties, at least in the area of public liberties or privacy. The biometric element then plays the role of a key which allows one to get into his home!

The CNIL has had the occasion to give a favourable decision on one of these applications. It concerned an experiment of electronic voting, where voluntary voters were issued with a microchip card which included the template of their fingerprint. The purpose of this recourse to biometric technologies was to ensure the identity of the voter and to establish presence sheets. No database of the voters' fingerprints was constituted, as authentication was based only on comparing the finger placed by the voter on a reader with the template of his fingerprint included in the microchip of the card.

2 – CONVERGENCE BETWEEN EUROPEAN DATA PROTECTION AUTHORITIES

Each European country has its tradition. But the European Directive of 24 October 1995 and its adaptation, carried out or in progress, in all the member States, undoubtedly contributes to a convergence of points of view. In this respect, all the authorities who have been consulted on developments in biometrics technologies insist on the principle of proportionality and the principle of purpose.

The Greek authority expresses its reserve concerning measures of controlling the presence of employees by fingerprint recognition but admits the recourse to such systems for reserved access installations.

The German authority has given a favourable decision on the introduction of biometric characteristics on identity papers in order to prevent their falsification, a project which saw the light after the attacks on 11 September 2001, provided that the data are stored in the microchip of the card for comparison with the owners fingerprints, and are not stored in a database. The German Parliament should be consulted on this project in view of its innovative character and of its importance.

The Dutch authority considers that when the biometric elements are not stored in a database, but only stored on an object exclusively available to the user (a microchip card, a mobile telephone, a computer, etc.) there is no reason for intervention. This position, which undoubtedly merits harmonisation on a European level, is not very far removed from the observations previously made by the CNIL.

D. Analysis of decisions by the CNIL on the subject

It has already been mentioned that the CNIL gave a favourable decision on an experiment of electronic voting by microchip card including the template of the fingerprint of its owner. The fact that no database storing the voters' fingerprints was constituted was stressed by the Commission in its decision.

When it concerns measures based on the constitution of a database, it appears very significant that the Commission have systematically given a favourable decision, or have not expressed particular reserve, when the database was constituted of templates of the outline of the hand, a biometric element which, unlike fingerprints, leaves no complete or detectable trace on the objects around us. This was the case of biometric recognition for the purposes of control of access and working hours of the cleaning personnel of the Louvre Museum (favourable decision 01-006 of 25 January 2001), of the access control implemented in a jeweller's shop (acknowledgement of notification of 12 February 2001), of the control of working hours of personnel treating handicapped persons at home (same date), of the control of working hours of cleaning personnel in a commercial centre at La Défense (acknowledgement of notification delivered in 2002). Therefore, whether the purpose of

the database was control of access or control of working hours, recognition by the outline of the hand has until the present day met with no reserve by the CNIL.

The Commission has also given favourable decisions, or has not expressed particular reserve, with regard to measures of access control based on the constitution of databases of fingerprints, when it was a question of an imperative requirement for security of the premises to be protected. The same applied to a control of access to high security areas of the Bank of France (favourable decision 97-044 of 10 June 1997), to the COGEMA at the Hague, where it concerned buildings for plutonium storage (acknowledgement of declaration of 17 November 2000), to the production areas of the Visa Card Group premises (acknowledgement of notification of 25 April 2001), and to production areas of microchip cards at the SAGEM (acknowledgement of notification of 25 April 2002).

On the other hand it has given unfavourable decisions, or decisions with reserve, when it concerned fingerprint databases for the purpose of controlling access to a school canteen (unfavourable decision 00-015 of 21 March 2000), or to all premises of academic halls of residence, when only the access to certain rooms which should be protected, such as those reserved for the storage of examination subjects before the date of the tests, appeared in this case to justify such a measure. These two decisions were taken for the reasons particularly of absence of any specific imperative requirements for security distinguishing these premises from all the others and for an obvious lack of proportion between the measure and the stated objective.

In the same manner, the Commission also gave negative decisions where fingerprint databases were constituted for the purposes of controlling working hours in a prefecture (unfavourable decision 00-057 of 16 November 2000), in an airline company (who finally gave up implementing the measure), or in a town hall (unfavourable decision 02-034 of 23 April 2002).

These decisions undoubtedly outline a doctrine which, at this stage, could be resumed as follows:

1. The biometric recognition technologies that are not based on storing the templates in a database give rise to no particular difficulty in terms of “data protection”, when the template is kept on the person (a microchip card) or on an apparatus of which he has exclusive use (a mobile telephone, a computer, etc.) and nowhere else.
2. On the other hand, when a database is constituted in the framework of a biometric identification measure, the chosen biometric element may have an incidence on our liberties and our privacy; that is the case when the chosen biometric element “leaves traces” in our daily lives (DNA, the fingerprint). In such cases, the control of purpose and proportionality may lead to the implementation of such databases being accepted when it is justified by a particular imperative requirement for security.
3. Failing such particular justification, and when a database of templates is constituted, the choice of a biometric element “leaving no trace”, such as the outline of the hand, the retina, voice recognition, etc., should be preferred to the proliferation of DNA or fingerprint files.

It remains that, far from any dogmatism, the CNIL wishes to pursue any useful reflection on the subject, in liaison with the professionals of the sector concerned and with its European opposite numbers in a concern for seeking the best possible balance.

E. Some more general reflections

Beyond the technique, beyond the wish of the concerned professionals to make their products more attractive or to better distribute them, beyond the concern of the administrations or the companies for making their premises, and sometimes their personnel, more secure, the biometrics technologies reveal three questions that we would be wrong to conceal, to disguise or to underestimate.

The first question which principally concerns the CNIL, and no doubt some others, is a question of privacy and personal liberties linked to the systematisation of the logic of traces, particularly of DNA and fingerprints, but also, soon, if it is not already the case, of our voice prints, of identification by odour, an emerging technology. With these technologies the world becomes an immense real memory (our traces), increased by a virtual world (the seeking and identifying of our traces).

The second question is linked to a weakening of the anonymous public space. Largely beyond video-surveillance, all the means of mobile technology blur the until now impervious distinction between the situations in which we are anonymous and those where we identify ourselves (a purchase by bank card, a telephone call we make from a mobile 'phone). Thus, between a situation of liberty and a situation of non-liberty, there is now much more gradation than distinction. The electronic bracelet placed on the ankle of the convicted person carrying out his sentence at home is only the most spectacular illustration of this phenomenon. But face recognition technologies associated with video-surveillance raises, for a larger number of persons concerned, some problems of the same nature with respect to the freedom to come and go or to the right to demonstrate on the public highway.

The third question is linked to the desire for disposing of several identities, at least virtual, as witnessed by the uses of the Internet, a world of pseudonyms, which no doubt contributes to the fragmentation of the digital identity. Similarly, and much earlier, the legitimate reticence concerning the inter-connection of, particularly, administrative files, encouraged a fragmentation of the administrative identity where our liberty lodges. But does this logic of fragmentation, or even dematerialization, not contribute to an increase in the importance of the biological identity?

As if the temptation to grasp, at the most basic level, an immutable identity was nourished both by our desire for liberty and by our fears that the identity of the Other is uncertain.