



Press Conference

Tuesday June 22, 2004

Contents :

Section 1

«Data processing shall be at the service of every citizen. It shall develop in the context of international co-operation. It shall infringe neither human identity, nor the rights of man, nor privacy, nor individual or public liberties.»

THE CNIL IN FIGURES	2
ACCESS TO POLICE FILES	3
BIOMETRY IN THE ERA OF SECURITY	4
THE GENETIC FINGERPRINT FILE (FNAEG)	6
LOCAL BIOMETRY : PRIORITY TO WHAT DOES NOT LEAVE TRACES	8
RESERVATION FILES FOR PASSENGERS BOUND FOR THE UNITED STATES	9
UNWANTED FAXES	11
THE FIGHT AGAINST SPAM	12
REMINDERS TO FINANCIAL INSTITUTIONS	13
« BLACK LISTS » OF CAR RENTAL COMPANIES	14
TRAVELLING TRACEABILITY	15
THE AUTOMATIC DRIVING OFFENCE REPORTING SYSTEM	16
« CYBERSURVEILLANCE » IN THE WORKPLACE	17
ELECTRONIC ADMINISTRATION IN THE NEAR FUTURE	18
FOUR MAJOR TECHNOLOGICAL CHALLENGES	20
LAST MINUTE	
OPINION ON THE PERSONAL MEDICAL FILE	21
« DID THEY READ IT ? » : WARNING BY THE CNIL	23

Contacts :

CNIL

21, rue Saint-Guillaume

F-75340 Paris Cedex 07

Phone : +33 (0)1 53 73 22 13

THE CNIL IN FIGURES

The CNIL's work remained stable in 2003.

Requests

6 136 requests in 2003, including :

- 3 567 complaints
- 1 163 requests for indirect access
- 1 102 requests for advice

Most often people come to the CNIL because they have difficulties exercising their rights, particularly their opposition right to be listed in a file or to receive advertising materials.

The business sectors that resulted in the highest number of requests are, in decreasing order : advertising materials, bank, work, telecommunications.

Audits

31 audits in 2003.

The CNIL increases its audit policy through a constant increase in the number of audits since 2000, through unannounced audits of organisations and through operations in specific business sectors.

Processings notifications

65,921 new personal data processings recorded by the CNIL in 2003.

As at December 31, 2003, the CNIL had counted 941,076 personal data processings since 1978.

Plenary sessions

68 opinions adopted in 24 plenary meetings, including :

- 9 notifications to the prosecution department
- 5 warnings
- 1 unfavourable opinion.

Since its creation, the CNIL deferred 35 files to the courts, issued 61 warnings and pronounced 99 unfavourable opinions.

And also in 2003

50,000 pages visited on www.cnil.fr a day, 3,000 visitors a day.

6,500 subscribers to the monthly newsletter launched in September 2003.

CNIL attended 220 events, meetings or conventions.

See 24th activity report, p. 7 to 21

ACCESS TO POLICE FILES

An analysis of indirect access right requests shows that increasingly, applications come to the CNIL after a non-renewal of an arm permit (including for safety agents employed by the RATP or the railroad police), a hiring denial (for instance in guarding and security companies) or a dismissal resulting from an unfavourable administrative inquiry.

Since the laws dated November 15, 2001 and March 18, 2003 on domestic safety, administrative inquiries conducted for access to some categories of public or private jobs, including in the area of security or defence, can result in police file consultation, including the STIC or JUDEX.

In 2003, the CNIL conducted 1962 checks, including 435 in the files of the police department of the Ministry of the Interior (STIC) ; 204 people were not in the files, but out of the 231 people reported as involved, 50 reports were deleted and 3 were updated, those 53 sheets accounting for 23 % of the total of all sheets submitted to the CNIL members.

A few examples of deletions :

- . A young person was listed in the police files since the age of 16 for the mere reason that he was carrying a pocket knife during an identity check.
- . An elderly person was listed as involved in an armed robbery and sequestration case, whereas she was the victim.
- . An individual was reported in a 20 year old swindling scam where he was a witness.
- . An applicant was reported in the STIC as involved in a use of drugs case. Actually, he has been questioned during the charging of a friend with use and sale of drugs because he shared the same apartment as the offender.
- . A person was listed as having been involved in a minor abduction case, while the minor had taken refuge at his/her place for one night.
- . An applicant was listed in a sex case at the time he worked as an educational assistant in underprivileged neighbourhoods. After the investigation, the claimant was found innocent.
- . A person was listed in a case dating back to 1998 mentioning his/her conviction to a 10 month driving licence withdrawal. Yet, a non enforceable ruling report had been issued on the ground of usurped identity.

See 24th activity report, p. 49

BIOMETRY IN THE ERA OF SECURITY

On a European level, initiatives have been taken to standardise the introduction of biometric data in visas, residency permits and passports. In France, the Act dated November 24, 2003 relating to immigration reformed identity check procedures for visa issuing and border checks rather substantially, by generalising the use of biometrics techniques. The Ministry of the Interior is studying an electronic identity card plan integrating fingerprints. These plans raise important issues in terms of personal data protection.

The CNIL is carefully following the work carried out in Europe to standardise the introduction of biometrics data (pictures and fingerprints) on visas and residency permits, and to establish a joint visa information system (VIS) allowing to identify visa denials and applications in one base.

On the CNIL's initiative, the group of European commissions responsible for data protection (« Article 29 Group ») should shortly express its thoughts on the draft regulations prepared in that area, specifically on the issues raised, in terms of data protection principles, by the creation of a central European biometrics data base (their opinion could be discussed at the group's meeting dated June 22, 2004).

In France, the November 26, 2003 immigration act provides for the right to take, memorise and process fingerprints as well as the pictures, not only on residency permit applicants and illegal foreigners but also of visa applicants « in order to protect the right to residency of legal foreigners and to fight against illegal entries and stays of foreigners in France ».

Consulted by the Ministry of the Interior, the CNIL expressed an opinion on April 24, 2003, on such provisions, considering that the memorisation and processing of fingerprints, due to the characteristics of the physical identification element and to the possible use of the developed databases, should be justified by absolute requirements in terms of safety and public order. It also said that given the magnitude of the databases that could be developed, appropriate guarantees were to be taken to ensure that individual rights and liberties were protected, particularly in terms of access to the bases, keeping times and data updating. The CNIL will be asked about the implementation order for those provisions.

That position was also formally restated by the CNIL in the first comments it sent to the Ministry of the Interior regarding the electronic identity card. That plan to revise identity cards would consist in replacing the current identity cards with a card with a microprocessor which, as part of the development of electronic administration, could be used to access teleservices. The card could include fingerprints, likely to be kept in a central base, like the pictures.

As a result, the CNIL asked the Ministry of the Interior that a precise list of argument be provide to it, specially on why and how the biometrics data would be used, whether it be direct reading of the identity card of the keeping of fingerprints in a central database.

As a reminder, when the CNIL expressed comments in 1986 on the plan for an inalterable identity card, it attempted to secure guarantees likely to prevent the issue of the new cards from resulting in a general individual check and to the development of a national population file. It had obtained from the Ministry of the Interior the assurance that no national fingerprint file would be set up, with fingerprint lists being kept in manual files kept by prefectures.

See 24th activity report, p. 26 and p. 82

THE GENETIC FINGERPRINT FILE (FNAEG)

The "Loi sur la sécurité intérieure" ("Domestic Security Act") dated March 18, 2003 broadened both the list of offences reportable to the national automatic genetic fingerprint file (FNAEG) and the list of people whose fingerprints could be included in that file or compared with its contents. The implementation decree for those provisions was published on June 2, 2004 based on the CNIL's opinion.

When asked an opinion about the draft State Council decree enacted in pursuance of section 706-54 of the criminal procedure code, the CNIL ruled that due to the importance of the double extension of the scope of the file, serious guarantees were required in order to prevent any uncontrolled, erroneous or abusive registering and any use of the file for purposes other than the ones for which it was created.

Indeed, as a reminder, when it was created, the FNAEG only included genetic fingerprints of people convicted for serious sexual offences. After the "Loi sur la sécurité quotidienne" ("Daily Security Act") dated November 15, 2001, the list of offences was broadened once to offences in connection with terrorism or damage to property, and a second time, by the Act dated march 2003, to the extent that the very nature of the FNAEG was changed, as it was initially designed to facilitate the identification and finding of sexual offenders, and now applies to almost all crimes and offences in connection with damages to property or injuries to people, as well as trafficking.

Regarding the broadening of the list of people concerned, the FNAEG had a similar evolution : initially, it was to identify the genetic fingerprints of people definitely convicted, but changes resulting from the "Domestic Security Act" dated March 18, 2003 now allow to register in the file the genetic fingerprint of individuals charged (whereas until now, their genetic fingerprint could only be compared with the content of the file, and could not be stored) and those of missing people, as well as, with their consent, those of relatives in the ascending or descending lines of these missing people. Lastly, the genetic fingerprint of people in police custody can now be compared (and not stored) with the content of the file.

When the draft implementation decree was reviewed, the CNIL secured a number of guarantees :

- The maximum storage time of information is twenty five years instead of the forty years initially planned ;
- The consent for taking biologic samples from the relatives in the descending or ascending lines of a missing person will be written down in a report ; in addition, their genetic fingerprint cannot be compared with the whole base without their consent ;
- The nature of the case requiring samples, used for statistical purposes, shall never appear during file consultations, nor be used as research criteria ;
- The decree implementation order will be submitted to the Commission, in particular for updating and deleting conditions ;
- The order formally specifies that the genetic fingerprints entered in the file should only be realised on the non-coding part of the DNA.

The Commission has also asked :

- Different storage times for information registered in the file, depending on the nature and seriousness of the offence, whether it be for convicted people or those against whom there are serious or converging signs that they are likely to have committed one of the offences mentioned in section 706-55 ;
- That the order should provide for no exception to the maximum information keeping time, set to twenty five years, for instance for people suffering from a mental or neuro-psychic disorder at the time of the offence, affecting their judgement or the control of their acts ;
- The deletion of information when the individual was cleared by the legal proceeding, in particular when the culprit of the facts the individual was suspected of is identified.

Those proposals were not followed by the Government.

See 24th activity report, p. 29

LOCAL BIOMETRY : PRIORITY TO WHAT DOES NOT LEAVE TRACES

The CNIL is still not in favour of the use of fingerprint databases by local authorities, schools and employers without an absolute security-related requirement.

The CNIL lately commented on several fingerprint recognition devices in various areas and confirmed its doctrine with regard thereto, which it has developed since 2000.

The Commission considers that fingerprints, unlike other biometrics data, leave traces that can be used for the purpose of people identification and that any fingerprint database is likely to be used for other purposes than its initial purpose. Only an indisputable security requirement may justify the setting up of such bases.

Conversely, the Commission believes that if the fingerprint is only stored in private material (smart card ...), the device is compliant with the Act dated January 6, 1978. The same applies to devices using biometrics that leave no trace such as hand or iris outline recognition.

That is why it expressed an unfavourable opinion about the use of an access control device for city roller park subscribers, relying on a central fingerprints base.

In the same way, the CNIL asked two schools to give up the fingerprint file that they set up to manage the access of their students to the school's cafeteria. Both school directors agreed to use another technique.

The CNIL has also issued an unfavourable opinion about the setting up by a hospital, of a fingerprint recognition device used to control work times, as the biometrics data were stored in a biometrics player, which employees have no control on, and not on an individual medium.

The Commission did express a favourable opinion on the use of an access control device for reserved security areas at Orly and Roissy airports, using a fingerprint recognition system. It was satisfied to have its proposal to keep the biometrics data on an individual access card (not in a central database, or a biometrics player) followed by "Aéroports de Paris".

See 24th activity report, p. 35

RESERVATION FILES FOR PASSENGERS BOUND FOR THE UNITED STATES

In pursuance of American antiterrorist laws, European airlines should, since March 5, 2003, provide American customs with access to the reservation files of passengers bound for the United States. After one year's negotiation, the United States and the European Union signed, on May 28, 2004, an international agreement providing a legal base to the transfer of such data. The CNIL and its European counterparts see the undertakings by the USA as insufficient.

American antiterrorist laws and their implementation texts have unilaterally provided for the requirement from all airlines flying to the United States to provide control departments at American borders with access to the reservation files of their passengers, referred to as "Passenger Name Record" (PNR), contained in their reservation system. Airlines that do not comply with the American customs' requests were threatened with sanctions as serious as landing denials.

Informed by the airlines, the CNIL and its European counterparts within the « article 29 » group (a European working group set up by Directive 95/46/CE) warned the governments, the European Commission and the public opinion about the unlawfulness of the data transfer to American authorities relative to private data protection.

The European Commission, in co-ordination with the members states, initiated negotiations with the American authorities, resulting in the United States agreeing to a number of undertakings aimed at ensuring an adequate level of « PNR » data protection.

Based on those undertakings, on May 17, 2004, the European Commission adopted a decision acknowledging that passenger data transferred to the US Customs and Border Protection Office received adequate protection. The adoption of that decision by the Commission resulted in the United States and the European Union signing, on May 28, 2004, an international agreement authorising passenger data transfers to American authorities.

The Commission's decision and signing of the international agreement took place in spite of the opinions issued by the European Parliament and the « article 29 » group that indicated that the American undertakings did not offer an adequate data protection level. With regard to that, the European Parliament may still bring the case before the Court of justice in order to have the international agreement or decision acknowledging the adequate data protection level cancelled.

The decision adopted by the Commission provides for a mutual data transfer system when the European Union or its members states will impose similar requirements for flights from the United States.

The guaranties obtained such as mentioned in the Commission's decision are as follows :

A smaller number of data collected and kept by the American authorities (34 categories of data are transferred),

Sensitive data providing religion or health-related information will no longer be provided or if they are, will be filtered and deleted later,

The data can only be used in the framework of terrorism and criminality prevention,

The data will be deleted after a maximum period of three years and six months, except for data consulted in the framework of specific investigation or manually,

The American authorities inform the passengers about the purpose of the transfer and processing and the name of the person in charge of the processing,

The individuals have a right of access and rectification,

The authorities in charge of data protection in the European Union have jurisdiction to assist people for complaints filed with the American authorities,

The sorting of data cannot be carried out by American authorities other than on a case by case basis and for agreed purposes,

The data transfer to other American or foreign governmental authorities will be on a case by case basis, and subject to notification to a designated European Union authority,

The Commission and representatives of data protection authorities will carry out a yearly review of the United States' compliance with their undertakings.

The CNIL and its European counterparts find these guarantees inadequate, for the following reasons :

- The list of data is out of proportion ;
- Sensitive data should not be provided ;
- The data transfer's purpose should only be terrorism prevention and some terrorism-related offences ;
- The keeping time is excessive ;
- A « push » transfer method whereby the data are selected and transferred by the airlines to the American authorities should be implemented, instead of the currently applied « pull » method (access by American authorities to the reservation systems and data collection)

See 24th activity report, p. 45

UNWANTED FAXES

On December 9, 2003, the CNIL reported to the Prosecution Department eight companies that sent unwanted faxes to individuals.

For many years, the CNIL has received complaints from individuals who received, generally within the framework of their work, unwanted faxes.

Doctors, lawyers, craftsmen, pharmacists, farmers, school principals and priests reported such intrusions in their private or professional life by that advertising method.

Every day, sometimes even at night, these people received advertisements on their faxes, which they usually used for private and professional purposes.

This advertising method has specific consequences : for instance, the fax machine of a craftsman, when busy receiving advertising, can no longer receive requests for urgent repairs ; more generally, the cost of the paper and ink is paid by the recipients.

Such an intrusion prompted the lawmaker, in July 2001, to subject the sending of advertisements to a fax user to his or her prior consent.

Since then, the principle is simple : direct advertising faxes are prohibited in France (like in all European Union member states) except to people who have expressed their consent to such advertising.

It was not before the publishing of a decree in the Official Journal dated August 6, 2003 that the fact of sending advertising by fax to an individual without his or her prior consent became punishable by a EUR 750 fine (art. R10-1 of the post and telecommunications code).

The Commission still receives very many complaints (708 in 2003), in spite of the decree having been published and the very many letters it sent to advertising fax sending companies, and on December 9, 2003, decided to report to relevant prosecution departments, eight companies that continued to send advertising faxes without first receiving the consent of the recipients.

The number of complaints addressed to the CNIL have consistently dropped since 2002 and most of them come from legal entities, which are not protected by the decree dated August 1, 2003 for which the Commission can only state its lack of jurisdiction.

See 24th activity report, p. 60

THE FIGHT AGAINST SPAM

The CNIL is committed in an all out fight against spam : application of anti-spam laws, awareness of internet users, adoption of codes of conduct and strong international co-operation.

Several countries have passed « *anti-spam* » laws including the United States, with the adoption of a federal law referred to as the « Controlling the Assault of Non-Solicited Pornography and Marketing Act », referred to as *Can Spam Act* effective since January 1, 2004. The American lawmaker chose to consecrate an opt-out system, unlike European provisions, which is less protective for European internet users.

In turn, France now has specific laws prohibiting *spam*, according to the CNIL's wish. The law for trust in the digital economy that is about to be enacted, reinforces the people's rights by subjecting the use of electronic mail in advertising campaigns to the prior consent of people (« opt-in » principle).

Work has been initiated with professionals for the implementation of this new legal regime. The CNIL is part of the dialogue and action group against *spam* launched by the government on July 10, 2003. The work of that group, which was officially installed on January 16, 2004, is co-ordinated by the Media development department. The CNIL leads the complaints and sanctions working group.

Indeed, for two years (« *spam box* » operation), the CNIL has undertaken an awareness action with prosecutors and specialist police departments. In this respect, it is relevant to underline that the CNIL will be a witness at the Criminal Court on June 25th at the trial of a company that it reported to the prosecution department on October 24th, 2002, after the « *spam box* » operation. The CNIL also supported legal actions initiated by internet access providers (see the sentence of May 5, 2004 passed by the Paris Business Court ordering a « spammer » to pay a EUR 22,000 fine for damages).

On an European level, the CNIL's purpose is to initiate an action co-ordinated with relevant European authorities to process complaints from internet users. The co-operation was made possible by the initiative taken by the European Commission which, in order to facilitate and co-ordinate information exchanges and best practices in the area of spam-related complaint processing, set up an informal on-line group including European authorities in charge of *spam* curbing. The CNIL leads that group for a period of 6 months.

Lastly, a world-wide co-operation action will be considered, i.e. where the main spam problem is located. The CNIL's main objective is to clean up the French market, before continuing its efforts in the world. However, the CNIL has frequent contacts with the US Federal Trade Commission and carefully monitors the work carried out by international organisations (OECD's *spam* workshop in February 2004, participation of the CNIL in the next workshop organised as part of the world summit on information society, held in Geneva from July 7 to 9).

See 24th activity report, p. 63

REMINDERS TO FINANCIAL INSTITUTIONS

In 2003, the CNIL issued four warnings to financial institutions that had not complied with regulations relating to the national loan repayment incident file (FICP), managed by the Banque of France.

The CNIL also issued two warnings to banks in 2004 for lack of security and confidentiality as regards clients information.

The action is continued in 2004, since the Commission issued five further warnings in March and June, to banks or loan institutions. This brings to 9 the number of institutions warned by the CNIL after an abusive entry into, or late removal of their clients from, the FICP file.

Banks sometimes use the FICP as a common « unwanted client » file : when in dispute with their client, they enter him or her on the FICP whereas he or she does not fulfil the conditions for being listed. Thus, this file, which was initially created to prevent individual overindebtedness, is becoming a means of pressure used by banks against their clients.

Institutions warned by the CNIL	Warning date
Banque française et commerciale d'Antilles-Guyane (BFCAG)	June 3, 2004
Caisse de Crédit Mutuel du Dauphiné (CAFIDA)	June 3, 2004
Caisse régionale de Crédit Agricole mutuel de Charente maritime – Deux Sèvres	June 3, 2004
Compagnie générale de location d'équipements (CGL – CGI)	March 25, 2004
Finaref	March 25, 2004
Crédit Mutuel du grand Cronenbourg	November 20, 2003
Crédit immobilier de France – Ile de France	November 20, 2003
Caisse régionale de Crédit Agricole mutuel du Nord	June 19, 2003
Fortis banque	April 24, 2003

The CNIL also sent two warnings on March 25, 2004 and June 3, 2004, to the Banque populaire Loire et Lyonnais and to the Caisse d'Épargne des Alpes, for not having taken all necessary precautions to ensure security and confidentiality to clients information. The Banque populaire Loire et Lyonnais had sent account statements to other people than the holders. One client of the Caisse d'Épargne des Alpes accessed another client's account, on the internet with his password and personal access code.

See 24th activity report, p. 157

« BLACK LISTS » OF CAR RENTAL COMPANIES

Following complaints addressed by people who were denied car rental due to their listing on a black list, the CNIL conducted audits with the main car rental companies. As a result, it has adopted a recommendation containing guarantees applicable to the creation and handling of such files.

Following complaints filed by people who were denied car rental due to their listing on a black list, the CNIL conducted audits with the main car rental companies, and their union, "le conseil national des professions de l'automobile" (CNPA), an organization which represents the whole of the professions of distribution and services involved in the car industry – rental branch.

The findings confirmed that files were set up to identify risk clients, as professionals want to defend themselves against people whose behaviour is likely to cause them a financial loss.

Thus, in order to restate the guarantees that such files should provide, the CNIL has estimated necessary to adopt, on March 11th, 2003 a recommendation relating to the management of risk people files by rental companies (see Journal officiel dated May 17, 2003).

The CNIL's main recommendations are as follows :

- Clear information to clients : people need to be informed of the possible entry of data resulting in denying them car rentals. Except in the event of lawful exceptions, any entry to that end should be notified to the individual ;
- Responsible entries by professionals : the decision to enter data resulting in denying a client car rentals should be made by the people responsible for checking the certain nature of the loss ; the reasons for the entry should be objective and opposable to the person (for instance, it is important to distinguish between reasons for the entry resulting directly from the individual, and those pertaining to the organisation he is an employee of), not apply any judgement of value or behaviour appreciation, and be relevant and non excessive ; the commission recommends taken measures in order to prevent homonym problems ;
- Regular information updating : the people in charge of the file should adjust the data storage time to the various reasons for entries, and establish regular data updating procedures.

These recommendations are roughly the ones that the CNIL applies or will apply to any other « black list ».

See 24th activity report, p. 187

TRAVELLING TRACEABILITY

An increasing number of public transportation networks use smart cards to store transport tickets and holder-related information. These devices, referred to as « ticketing applications » memorise the transport of users and raise concerns with regard to both the freedom to come and go and the right to privacy.

Public transportation modernisation has prompted many companies to offer their users new transport tickets, based on the use of nominal magnetic or smart cards, in order to facilitate passenger access and travels and offer additional services.

The CNIL has on many occasions commented on such devices, including in the framework of its investigation of the case submitted by the RATP for the « Navigo » ticket pass, and has conducted controls of collective transportation companies using similar applications.

The use of such nominal cards results in collecting information pertaining to the routes of users accessing and sometimes exiting the network, as well as during connections ; The system memorises, on the card and in the central computer of the transportation company, the dates, times and places of passage, as well as the card number.

As a result, the trips of people using such cards can be reconstructed and are no longer anonymous, and the processing of such information is likely to affect the freedom to come and go, as well as rights to privacy.

The CNIL has decided to issue a recommendation so as the collection and processing of personal data by public transportation companies to comply with the principles of the January 6, 1978 Privacy Act.

The CNIL's recommendations include a recommendation that user travel-related data should not be used in any form allowing to identify the user, except in the framework of fraud prevention, for the time necessary for detecting the fraud, such time not exceeding two consecutive days.

The development of this recommendation gave place to the consultation of the Union for Public Transports (UTP), the French Group of Authorities in charge of Public Transport (GART) as well as the Ministry of Transports, in order to collect their observations.

See 24th activity report, p. 136

THE AUTOMATIC DRIVING OFFENCE REPORTING SYSTEM

The CNIL issued a favourable opinion in 2003 on an experimental automatic driving offence reporting system implemented in pursuance of the road violence Act. However, the CNIL requested that access to the picture of the vehicle be possible on receipt of the fine notice.

The CNIL was asked by the Government for its opinion on the draft order instituting an experimental system aimed at automating the control and sanctioning of some driving offences.

Does the system breach article 2 of the January 6, 1978 Act, according to which « No judicial decision involving an appraisal of human conduct may be based on any automatic processing of data which describes the profile or personality of the person concerned » ?

It should first be underlined that that the draft order is the translation of the Act dated June 12, 2003 reinforcing the prevention of driving offences, which provides that a fine notice « may be sent after the finding of a breach of the driving code by an approved automatic control device ». At any rate, the automated processing of driving offences does not provide a definition of the profile or personality of the offenders, because it is aimed at no specific category of drivers.

In its opinion, the CNIL insisted on human involvement in a strongly automated process, by making sure that the offence reports are approved by police officers, and by requesting that the national processing centre be placed under the supervision of the relevant Public Prosecutor.

The CNIL has not issued any objection to the merger of the offence file and of the national licence plate file in order to identify vehicle owners whose licence plates are noted during a check.

Similarly, it agreed that the address change file of the Post could be used to check the current address of the owner of the vehicle. Indeed, the CNIL acknowledged that the consultation would be limited to those people indicating to the Post that they are not opposed to their address being disclosed.

However, the CNIL was particularly careful about access conditions for people to their data, including the digital picture of their vehicle. The CNIL judged that the holder of the licence plate certificate ought to be able to access any information about him on receipt of the fine notice, including the part of the picture showing the driver.

A CNIL delegation went to the management centre's premises in April 2004 in order to assess the system operating methods and the guarantees used at the various phases of the computerised processing. Indeed, the CNIL will shortly have to pronounce on the extension of a still experimental system.

« CYBERSURVEILLANCE » IN THE WORKPLACE

Controlling the use of information technologies, specifically the internet, is a current issue for the CNIL

For several years, the CNIL has been pleading for a balance to be found, in the area of the use of information and communication technologies, including the internet, in the workplace, between the legitimate interests of employers and the necessary respect for employees' rights and privacy.

After publishing the report on « cybersurveillance in the workplace » (2002), the CNIL led several information projects towards companies and public authorities in order to check the compliance with its instructions. It also carried out a review of applicable texts and precedents.

Its in-depth work resulted in the publishing, in March 2004, of an updated version of its « cybersurveillance » report, available at www.cnil.fr and from "La Documentation française" Publishing.

In this last version, the CNIL discussed the change in the labour code (section L.412-8) which now officially provides unions with the right to use the intranet and e.mail system of their employers subject to a company agreement.

With regard to that, the CNIL stated the precautions to be taken :

- not use the electronic address files for other purposes than the union's communication,
- inform the employees of such use, so they can express their opposition to the sending of any union message to their professional electronic mail box,
- ensure the confidentiality of messages exchanged with the unions.

In addition, the CNIL noted an important ruling by the Judicial Supreme Court specifying that unnotified personal data processings are not binding on employees.

In this ruling dated April 6, 2004 (*see* www.cnil.fr), the Judicial Supreme Court indicated that if a badge-based personnel arrival and departure control system was not notified to the CNIL, the employer could not punish an employee refusing to use that system, even though company rules require personnel to do so, and that the existence of the system was notified to the employees.

Thus, it is reminded by the judge that any individual control of employees' work using automated systems should be notified to the CNIL.

See 24th activity report, p. 225

ELECTRONIC ADMINISTRATION IN THE NEAR FUTURE

The Commission is following with particular attention major electronic administration projects. It has examined at the beginning of the year the Government's electronic administration plan, ADELE.

In addition, the CNIL was asked about the provisions of the second bill authorising the Government, to simplify the law by way of decrees, currently debated by Parliament. The purpose of that text is to initiate a clear legal framework to ensure the development of teleprocedures and reinforce the security thereof; it also provides for the setting up of a "personal administrative area", an administrative data storage system provided to the user, and for a single address change service.

In order to develop economic administration in a trusting climate, the CNIL emphasises four principles, broadly reproduced in the ADELE program.

Proportionality

Electronic administration involves multiple interconnections between the various agencies, to better share information and simplify various formalities. The CNIL reminds that each of those interconnections and the setting up of central databases should be justified and really simplify administrative procedures. Each file connection plan should be specifically reviewed by the CNIL for it to appreciate its purposes.

Transparency

Transparency as regards personal data collection and exchange is one of the principles stated in the ADELE program. That principle is also championed by the CNIL. The administration should keep the user informed as to how his or her data can be updated or rectified, and about the means available for accessing his or her administrative information on line and check the accurateness of his or her administrative situation. Personal data exchanges between administrations are subject to the citizen's consent except when such exchanges are required by law.

Graduated security

It is obviously necessary to ensure anonymity for procedures that do not require the citizen to disclose his or her identity. When the identity needs to be checked, the technical means used should be adjusted to the type of procedure. In some cases, not in all, encryption or even electronic signing are necessary.

Multiple identifiers

One of the objectives of the ADELE program is to enable citizens to access multiple services and targeted information about them on a single Website. The program rules out the concept of the use of a single identifier. That position is similar to the CNIL's : one identifier for each sphere, no general use of a national identification number. However, the future identification systems should not result in a "de facto" centralisation. The CNIL will review each of the various identification options under consideration.

Within the coming months, the CNIL will have to review the concrete implementation of the ADELE program through projects that raise many issues.

Those issues include :

- The « address change » plan : what information will be recorded and how long ?
- The « daily life card » : what assignment and updating methods ?
- The "personal administrative area plan" : how can the user control the access to his or her information ?

See 24th activity report, p. 77

FOUR MAJOR TECHNOLOGICAL CHALLENGES

Technological evolutions are increasingly structuring personal data protection. The CNIL has identified four major challenges (cryptology, anonymity, biometrics, contact-less) and two significant issues (the future of internet and alternative technologies referred as PETs) which constitute its work programme in 2004-2005

Cryptology

Data securing through encryption is still not commonplace, even if technical proposals exist for controlling intellectual property rights or PC platform protection.

Anonymity and personalisation

How to conceal oneself to navigate around networks and make payments without circulating personal data ? That is the issue of anonymity.

How to access personalised services with an authenticated identity in one single operation ? That is the issue of personalisation.

Biometrics

The development of biometrics and its use for identity cards pose the problems of card security through means of electronic signing and of database interconnection.

Contact-less and geolocating

Cell phones, Wi-Fi and object radio-identification are technologies to be monitored closely. Indeed, a cell phone can be used to locate people even when the phone is on stand-by. With Wi-Fi everyone can become an access provider, unbeknown to him. RFIDs are used to identify or to spot an object, which, as a result, becomes a personal identifier.

The future of the internet

What freedom tomorrow on the internet when security become the main objective ?

The technological alternative

Could some technologies be more efficient than the law ?

See .file « Technological challenges for data protection »

OPINION ON THE PERSONAL MEDICAL FILE

Asked by the Government about the health insurance reform bill, the CNIL, at its meeting dated June 10, 2004, admitted that health insurance beneficiaries are not really free to deny access to their personal medical file, but requested appropriate guarantees to protect the private lives of individuals and ensure data confidentiality.

The health insurance reform bill provides for a personal medical file for each health insurance beneficiary, which will be stored on the internet and will include data collected or produced during prevention, diagnosis or care activities.

The reimbursement of procedures and services by the health insurance will be subject to the health professional's access to the personal medical file.

Because health data are part of the private life, they should be the subject of specific protection. Because of that and except in the event of legally required disclosures for public health interests, the CNIL has always included, among the guarantees likely to provide such protection, the need for the person's consent to the sharing of medical data.

In addition, section L.1110-4 of the public health code, in its text contained in the March 4, 2002 Act relating to the rights of patients, states the right of any person handled by a professional, and establishment, a health service or any other organisation taking part in prevention and care to privacy and to the secrecy of his or her information. That section also specifies that several health professionals can exchange information relating to a person in order to ensure constant care, except if the person opposes thereto.

The Commission observes that in accordance with the above-mentioned requirements, the bill by referring to the provisions of section L.1111-8 of the public health code, implies that the setting up of the personal medical file relies on the consent of the person. However, to the extent the level of reimbursement of procedures and services is linked to the health professional access to the file, it appears that the consent is not totally free.

Regarding health-related data, article 8 of directive 95/46/CE dated October 24, 1995 provides that they cannot be processed except in some circumstances such as firstly, the formal consent of the individual. It also provides that, subject to appropriate guarantees, member states can provide for other exceptions in their national laws, for a relevant public interest grounds.

The Commission believes that the provisions of the bill instituting a personal medical file and linking the reimbursement of care to the health professional's access to that file are justified by important public interest grounds, which, in the very terms of the text, are « co-ordination, quality and continuity of care » and improvement of the « relevance of the resorting to the health care system », the whole project being aimed at protecting the health insurance system.

However, it reminds that under the terms of section 8 of the above-mentioned directive dated October 24, 1995, the exception possibility is subject to the introduction of appropriate guaranties.

Thus the Commission believes that the law should be complemented by a specific statement indicating that the data likely to be stored in the personal medical file are covered by professional secrecy such as defined in the criminal code and that anyone obtaining or attempting to obtain disclosure thereof in breach of the provisions of this article will be prosecuted, as well as anyone changing or attempting to change the information written in the file.

The Commission also believes that since an access to the personal medical file provided by the internet network is envisaged, such a use, because of the data disclosure risks, cannot be accepted unless extremely strict security standards are imposed on both health professionals and organisations storing the data.

With regard thereto, the principle of the prohibition of any sale of directly or indirectly nominal health data should be included in the law.

With regard to informing people, the CNIL states the need to inform clearly the person on the setting up, updating, using methods for his or her medical data, and also about the conditions in which he or she may access such data. Identification and authentication methods, including for the use of the health professional card, should be defined.

« DID THEY READ IT ? » : WARNING BY THE CNIL

The CNIL considers that the use of the new e.mail monitoring service « Did they read it ? » may be illegal in France.

An American company « Rampell Software » has offered, since the end of May, a new e.mail monitoring service called « Did they read it ? ». That device is used by any internet user, subject to payment of a fee, to find out whether the recipients of his e-mails read them, when, how many times, how long, if they forwarded them to other people and from which message server. It is also used to find out what browser is used by the recipient, as well as his operating system.

The process takes place unbeknown to the recipient of the e-mails. Unlike the acknowledgement of receipt provided by standard e.mail softwares, the recipient cannot accept or refuse to return the information to the « Did they read it ? » subscriber. He is not even informed.

By principle, the CNIL can only express the most formal reserves about such a process. Indeed, it is a personal data collection, as detailed information is recorded and sent, pertaining to the « behaviour » of an e.mail recipient. Such a processing, carried out unbeknown to people concerned is against data protection rules, and more specifically against section 25 of the Act dated January 6th, 1978 relative to information systems, files and liberties, which prohibits the collection of personal data carried out by any fraudulent, dishonest or illegal means.

The CNIL reminds that failure to comply with those provisions can result in a five year prison sentence and a EUR 300,000 fine (section 226-18 of the criminal code).

As a result, the CNIL draws the attention of French companies, administrations and more broadly, of the public, to the fact that any subscriber to « Did they read it ? » in France may be prosecuted.