



# Press Conference

June 26, 2003

Summary :

- **The CNIL at the Service of Citizens.....2**
- **The CNIL in Figures.....3**
- **Police Files in France since the New Home Security Act .....4**
- **The Explosion in Requests of Access to Police Files .....5**
- **Cases referred to the Judicial Courts and Follow Up .....6**
- **Disclosure to the American Administration of Reservation Files for Passengers to the United States .....7**
- **Storage and Use of Credit Card Numbers by Distance Selling Companies.....9**
- **Opinion of the CNIL on the Bill relating to Electronic Communications .....10**
- **The Results of Operation “SPAM BOX” .....11**
- **The PREVENTEL File : Numerous Complaints in 2002 but Clear Improvement in 2003 .....12**
- **Black Lists: “Bad Debtors” and “Frauds” on Record .....13**
- **Electronic Voting .....14**
- **E-Government Issues : more topical than ever for the CNIL.....15**
- **Surveillance of Diseases Subject to Obligatory Notification: Anonymity now guaranteed .....16**
- **The new Population Census .....17**
- **Implementation of The European Directive on Data Protection of October 24, 1995 .....18**
- **Last minute! The CNIL issues Warnings to Two Major Banks.....19**

## *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 AT THE SERVICE OF CITIZENS

---

**The CNIL is above all an institution at the service of citizens: with more than 5000 complaints received in 2002, the CNIL's mission of information on the law of January 6, 1978 and its mission of assisting individuals in the exercise of their rights are daily. Numerous problems as to how some data controllers apply the law are thus solved thanks to its intervention.**

---

Some examples from a few sectors to illustrate this.

- Credit : the CNIL intervenes in order to obtain from banks or credit institutions the deletion of information related to individuals that have been wrongfully registered in the national consumer credit negative file (FICP) managed by the Bank of France.

*See 23<sup>rd</sup> annual report, p. 105*

Mr F. was registered in the FICP by his bank more than seven years after the bank noted the default payment. The CNIL intervened to obtain the deletion of his record.

Mrs D., who was late in the reimbursement of one of her credit instalments, rapidly adjusted her accounts. Her bank, however, maintained her registration in the FICP for 18 months after settlement, and did not erase information relating to her until the CNIL had intervened.

- Telecommunications: The CNIL helps persons registered in the "Preventel" file.

*See 23<sup>rd</sup> annual report, p.113*

In January 2002 Mr G. cancelled his cell phone subscription. His operator informed him that he owed the sum of 120€ for the two months' notice remaining. Mr G. contested this notice and, consequently, the sum due. Mr G. then received several reminders from his cell phone operator, which registered him in the Preventel file but, on the other hand, he received no reply to his letters of objection. He contacted the CNIL which intervened. The operator, finally, recognised that its latest general conditions did not apply to Mr G.'s contract, cancelled the debt and removed his registration from the "Preventel" file.

- Marketing: the CNIL acts in order to limit the drift towards "too" personalised publicity.

*See 23<sup>rd</sup> annual report, p .60*

Mr D. regularly calls Algeria. His telephone operator's commercial agency, which had analysed his use of the telephone, sent him an invitation proposing a more favourable package for communications to Middle East and North African countries. It took advantage of the letter to wish him "a happy Ramadan". The Commission called to order the operator, which, quite obviously, may not deduce the religion of his clients from their telephone communications..

Mr F. registered on an Internet site of online games and indicated that he was single. Some time later he received from an insurance company some publicity boasting the characteristics of the "first insurance contract specifically conceived for the homosexual community" Investigation of this complaint produced evidence that the Internet site manager had sorted his clients according to whether or not they were single, then he had edited address labels which he made available to the insurance company. The CNIL intervened to demand that the measures of the law of January 6, 1978 be respected.

## THE CNIL IN FIGURES

---

**In 2002 all the figures concerning requests to the CNIL showed an important increase. These figures prove how much French citizens are keen to have their data protection rights respected and enforced. They also confirm that they do not hesitate to denounce the abuses they are, or feel they are, victims of.**

---

**Total requests : global increase of + 38%**

**42%** The year 2002 has shown a real explosion of all types of requests to the CNIL : **5076 complaints against 3574 in 2001, i.e. + 42% in 2002 compared with 2001. Requests for indirect access to police and security files increased by + 51%. All in all, requests globally increased by 38%.**

The most frequent motive for complaints concerns exercising one's rights, and particularly the right to object to one's data being processed or to receive commercial solicitation. The sectors of activity which gave rise to the highest number of complaints are, in decreasing order : commercial solicitation (see chapter 2), the banking sector (see chapter 5), privacy issues at the workplace, telecommunications (see chapter 5).

**32%** The significant growth (+ 32%) in requests for extracts from the « file of files », i.e. the CNIL's database registering all the forms of notified or authorised processing of data, also shows the citizens' interest in knowing the use which is made of their personal data.

**Since 1978 the CNIL has received more than 12.600 requests for advice and more than 41.270 complaints (as of 31/12/02).**

### **A reinforced audit policy**

Wishing to intensify its investigation policy, the CNIL multiplied its decisions to carry out audits in 2002 (52 in total). This figure, which is twice as high as the previous years, shows the will to anticipate the transposition into national law of the European directive 95/46/EC of October 24, 1995<sup>1</sup> which will lead the CNIL to carry out more inspections on the spot.

### **Other relevant figures**

- Since 1978 the CNIL has referred 25 cases to the judicial courts and issued 51 warnings. For 2002 only the CNIL referred 7 cases to the public prosecutor and issued 2 warnings.
- As of December 31, 2002, the number of processings registered by the CNIL since 1978 was 875 155, including 54 128 new requests of prior procedures for the year 2002.

***See 23<sup>rd</sup> annual report, pp 12-15***

---

<sup>1</sup> The bill ensuring this implementation was given its first reading in the National Assembly in January 2002, just before the interruption of work by Parliament and the end of the eleventh legislature. The Senate did not examine it in first reading until 2003

# POLICE FILES IN FRANCE SINCE THE NEW HOME SECURITY ACT

---

**Although it was not formally consulted by the Government, the CNIL considered necessary to inform both the Government and Parliament of its opinion<sup>1</sup> on the provisions of the home security bill which concerned police files and the national file of genetic fingerprints.**

While it regretted not being formally consulted on the issue, the CNIL, in its session of October 24, 2002, considered it as its duty to publish its main comments on the articles of the bill which pertained to its competence.

On the one hand, the CNIL acknowledged that, in accordance with its longstanding recommendations, certain indispensable guarantees concerning central police files, such as the national Police STIC file or its equivalent in the national Gendarmerie, the JUDEX file, would now be framed by law. The following guarantees were consequently implemented :

- control by the public prosecutor with local jurisdiction over the processing ;
- strict definition of the persons implicated, in line with the Criminal Code provisions;
- implementation of retention periods of the processed data;
- reinforcement of the principle of update, and in certain conditions, of deletion of nominative data concerning both the persons implicated and the victims.

**On the other hand, the CNIL recalled the position which it had already affirmed in its decision of December 2000 on the STIC on the risks implied by the new possibilities of checking police files for the purposes of administrative inquiries : such an extension risks turning these files into parallel criminal records without being subjected to neither the guarantees, nor the methods of control currently in place for the national criminal record.**

The CNIL also noted that the scope of the National File of Genetic Fingerprint (so-called FNAEG) was substantially modified, both in relation to the offences registered and to the persons concerned. It considered that such an extension required that new guarantees should be put into place, notably concerning the conditions of registration of information into this file and the conditions of storage and deletion of the data. It considered, in particular, that systems of automatic deletion of data should be provided for, which would operated when a procedure is closed and when the person concerned is cleared, particularly in the case of acquittal or discharge. It was not followed on this point.

The CNIL's opinion will be requested on two decrees of application of the Act concerning police files. The CNIL considers that it should also be consulted on the decree that will determine the categories of employment and functions for which an administrative inquiry may give rise to a consultation of police files.

*See 23<sup>rd</sup> annual report, p.22*

---

<sup>1</sup> The text on the position of the CNIL, dated October 25, 2002, can be found in the « Actualité » column on the Commission's web site ([www.cnil.fr](http://www.cnil.fr)) and on page 203 of the 23<sup>rd</sup> annual report.

# THE EXPLOSION IN REQUESTS OF ACCESS TO POLICE FILES

---

Since its creation in 1978, the CNIL has received more than 7.500 requests of indirect access to police files, which have led to more than 12.500 investigations. The number of these requests keeps growing every year, to a point where in 2002 one may speak of a real “explosion” of requests.

---

According to the law of January 6, 1978, any person has the right to request of the CNIL that verification be undertaken by a member of the Commission on any information concerning him or her which might appear in files relating to the security of State, defence, and public safety. No police file can escape investigation by the CNIL.

**+51%** In 2002 the Commission received 1264 requests which have given, or will give, rise to more than 2500 investigations (as one request may concern several files), i.e., **an increase of +51% compared with 2001.**

**94% of the verifications concern Home Office files, and in particular Intelligence Service files (“Renseignements généraux”).** In 2002, **1012 such investigations** were carried out in Intelligence Service files : 77% of the applicants were not on file, and of the 236 applicants on file, 85% obtained permission to consult their file.

As the law now authorises the consultation of police files for the purpose of administrative enquiries, notably to fill certain jobs in the areas of security and guarding, the CNIL more and more often receives requests for verification.

In general, the applicants have been refused employment or accreditation for certain functions, they have applied for a job in the public sector, or, after having been questioned by the police, they wish to verify that they are not listed in police files. The media coverage of these procedures has also driven numerous persons to request verification by the CNIL.

**37%** **The investigations carried out by the CNIL into police files and, in particular, into the system of established infringements (the so-called STIC: système de traitement des infractions constatées), have in 37% of the cases led to updating or even deletion of erroneous, or clearly unjustified, mentions.**

An applicant was refused a training course in a judicial court on the basis of his registration in the STIC as being “implicated” in a case of theft of a moped when, in view of the retention period laid down by the decree of July 5, 2001, this information should no longer have appeared in the system. As a result, the CNIL obtained from the police services that the corresponding record would be deleted, and they informed the court in question, in order that the application be re-examined.

An applicant was listed in the STIC after being held in custody, as a witness, in an investigation concerning a case of traffic in forged currency in 1984. On demand of the magistrates of the CNIL, the police deleted the record of this person.

*See 23<sup>rd</sup> annual report, p.28*

## CASES REFERRED TO THE JUDICIAL COURTS AND FOLLOW UP

---

**In 2002 the CNIL referred seven cases to the public prosecutor. Three of these cases were discharged without follow-up, the other four have, to date, not given rise to any procedural decision, whether of discharge or of judicial investigation.**

---

*“Someone secretly loves you and asked that we should tell you; find out who fancies you by calling 08 ... .. 1,35€/call + 0,34€/min”*. The massive dispatch of this SMS for the sole purposes of pushing persons to dial a number so as to charge them for calling and of collecting mobile telephone numbers in order to file a database, was referred to the public prosecutor by the CNIL on June 27, 2002. The CNIL considered, in particular, that the companies at the origin of this dubious and irregular commercial practice had collected personal data in an unfair manner. To date, no formal judicial decision has been handed down on this case.

On July 8, 2002 the CNIL referred to the courts the case of an Internet-marketing company for setting up a database registering the political opinion of Internet users by means of proceeding to a poll carried out between the two presidential ballots. The company has alleged that the answers to the poll should have been treated anonymously, which appeared not to be the case. Although this case was discharged by the court of Nanterre on January 20, 2003, it has just been “taken over” by the Public Prosecutor of the Versailles court.

On July 10, 2002 the CNIL initiated the so-called “Operation Spam Box”, which gave the possibility to Internet users to transfer unsolicited electronic mails received on their mailboxes to an email address opened on the CNIL’s server. This operation was concluded on October 24, 2002 when the cases of five companies were referred to the courts for judicial follow-up. Two of these cases were discharged by the Prosecutor of the Paris court but to date, the other three cases have not given rise to any formal legal proceedings.

The principle of criminal procedure known as “advisability” of legal proceedings” grants public prosecutors with the liberty not to engage proceedings in cases where facts yet can be qualified as a criminal offence. The CNIL, naturally, does not contest this. The decisions to discharge three of the cases referred to the Courts by the CNIL show, for at least two of them, how difficult it can be to identify persons that have infringed data protection rules. This is particularly the case with companies bearing different corporate names, which are often located abroad, which carry out irregular spamming operations.

But these decisions, as well as the official statistics of the Ministry of Justice (2 sanctions were pronounced in 2001 for infringement of the Data Protection Act), highlight the need for the CNIL, the police services, and the services of the public prosecutor to continue their exchanges, in order for this complex area of criminal law not to be completely sacrificed in overburdened courts.

# DISCLOSURE TO THE AMERICAN ADMINISTRATION OF RESERVATION FILES FOR PASSENGERS TO THE UNITED STATES

---

**Since March 5, 2003, European airline companies have given American customs access to reservation files for passengers flying to the United States. The guaranties already obtained by the CNIL and its European counterparts are still insufficient to ensure adequate protection of passengers' privacy.**

---

The American anti-terrorist legislation and regulations provide for the unilateral obligation of any airline providing flights to the United States to give the controlling services at the American borders access, on request, to the reservation files of their passengers, the "Passenger Name Record" (PNR), contained in their reservation system.

The reservation dossiers are filled in by travel agents in order to give the airline companies the information necessary to provide the services requested by passengers. These files may, therefore, systematically include the identity of the passenger or of passengers travelling together, the complete itinerary, the personal or invoicing address, the telephone number and the means of payment, and in certain cases, the charge card number, medical information or information about diet preferences of a religious nature.

Airline companies which do not comply with the demands of the American customs might be subject to sanctions going as far as landing refusal.

Informed by the airline companies of the threats hanging over them if they did not comply before the end of the year, the CNIL and its counterparts within the "article 29" group (the European group instituted by the 95/46/CE directive) agreed on an opinion, dated **October 24, 2002**. Whilst recognising that certain exemptions from the purpose principle can be legitimate in the framework of prevention of terrorism, the opinion raises the question of sensitive data and of proportionality. Thus the governments, the European Commission, and public opinion have been made aware of an international issue, in which passengers and airline companies cannot be left alone faced with the American demands.

In co-ordination with the Member States, the European Commission has established a dialogue with the American authorities on both a technical and a political level. In order to obtain a certain number of guarantees, the deadline given by the American administration for carrying out data disclosure has been postponed twice.

Based on the first American commitments contained in a common declaration, dated **February 17, 2003**, the airline companies finally granted the access to data demanded by the American administration on the 3<sup>rd</sup>, and last, deadline date of **March 5, 2003**.

**The guarantees obtained notably concern non-access to information about passengers not going to the United States, and special protection or deletion of any sensitive data collected.**

The list of questions raised by the data protection authorities, with a view to limiting the required data transmissions to proportionate content and modalities, and the pressure exercised by the very critical resolution voted by the European Parliament on **March 13** this year have, however, led the American authorities to propose a list of undertakings on **May 22, 2003**.

Nevertheless, as acknowledged by the European Commission itself, this American document cannot yet serve as the basis for a satisfactory permanent framework, while its rapid adoption would be necessary.

In its opinion of **June 13, 2003** the “Article 29” group recommends improvements on the following points:

- the purpose of such data transfer must be limited to the prevention of serious acts of terrorism ;
- if its transfer would be acceptable, the data must be limited to identity, itinerary and mode of travel organisation, excluding any data of a sensitive or economic nature, or relating to particular services requested by the passengers ;
- transmission of data must be carried out by the companies themselves and not by direct access by the American authorities to the reservation systems, (“push” instead of “pull”) ;
- the retention period duration should be limited to a few weeks or months instead of the 15 years as planned by US authorities ;
- an independent body must be able to rapidly receive and deal with complaints by passengers (right of access and correction) and ensure control of any processing intended to detect “undesirable” persons and of persons to be subject to specific control according to standard profiles.

**While awaiting a satisfactory solution, the companies must inform passengers and implement the means to transmit the data by themselves in order to remove data to be established as excessive.**

# STORAGE AND USE OF CREDIT CARD NUMBERS BY DISTANCE SELLING COMPANIES

---

**Following a wide consultation of the main professional federations and the public authorities concerned and a call for public contributions, which triggered 2300 reactions from consumers, the CNIL published a recommendation on June 26, 2003 concerning the storage of credit card numbers in the distance selling sector.**

---

The question of means of payment, particularly on the Internet, still gives rise to numerous interrogations by consumers and certainly remains a key element in the development of e-commerce in the future.

During the year 2002, the CNIL received a growing number of complaints from consumers concerning the storage and use of their credit card number by companies specialised in distance selling, whether by telephone, by post, or on the Internet.

*For example, some persons, when booking a hotel room by phone, discovered that their banking information has been stored since their last visit to the hotel. In other cases, some debits were ordered by certain Internet access providers without justification, although they had no more relations with the clients concerned, but whose banking information was still activated in their commercial database.*

For online e-commerce sites, the issue revolves around the conditions of confidentiality under which credit card numbers are stored on the companies' server and around the new uses of the credit card number, such as the development of e-portfolios.

**The CNIL recommends that, when a credit card number used for commercial identification purposes is stored beyond the time needed to carry out a transaction, it should be subject to the consent of the person concerned.**

Concerning the fight against payment fraud, and in order to take into account the legal specificity of payments at a distance, the recommendation recalls the conditions under which a distance selling company may keep a record of acts which have been detrimental to his interests for the purposes of internal management.

The CNIL also proposes several practical recommendations, such as having recourse to technical procedures allowing irreversible encryption of credit card numbers as soon as the transaction has been carried out, in order to improve the security of credit card databases, in particular when these are accessible on the Internet.

In order to favour e-commerce development together with respecting people's privacy, the CNIL considers, finally, that data controllers should promote the use of alternative secure means of electronic payment that would guarantee the anonymity of the payments made by their clients.

# OPINION OF THE CNIL ON THE BILL RELATING TO ELECTRONIC COMMUNICATIONS

---

**Like other regulatory authorities (namely the Telecom Authority and the Audiovisual Council), the CNIL gave its opinion on the bill relating to electronic communications. This opinion was the occasion for the CNIL to confirm some of its positions, in particular that subscribers should be able to register on the so-called “red list” (i.e. refuse to appear in a public directory) free of charge. It also reaffirmed that it will be very attentive to the storage conditions of data held by electronic communications operators.**

---

The CNIL was formally requested to provide its opinion on the bill relating to electronic communications which is to implement the European directives collectively known as the “telecoms package”.

The bill essentially modifies the law of September 30, 1986 on freedom of communication and, more specifically for what concerns the CNIL, the Code on post and telecommunications (P&T). Two sections directly concerning personal data protection have been created in the Code; the first relating to “*Directories and inquiry services*”, and the second to “*Privacy protection for users of networks and telecommunications services*”.

Concerning directories and inquiry services, the Commission reasserted its constant positions:

- on the one hand, the right to refuse to appear in a directory (registration on the red list) should be exercised free of charge;
- on the other hand, the regulatory authorities should explicitly acknowledge the specific right to oppose being listed by reverse search functions in directories.

These recommendations had already been expressed in the decision by the CNIL on the project of decree relating to the so-called “universal directory” (including both fix and mobile telephony numbers).

Concerning the privacy protection for users of networks and telecommunications services, the bill specifies the conditions under which localisation data may be stored by electronic communications operators and used to supply value-added services. On this latter point, the bill introduces in French law the principle of prior consent as provided by the European directive of July 12, 2002. Although the bill does not directly deal with the determination of retention periods of data as sensitive as that of localising the users of an electronic communications service - two coming decrees should specify this point -, the CNIL has already stated the importance it attaches to this question.

*See 23<sup>rd</sup> annual report, pp 139 and 206*

## THE RESULTS OF OPERATION “SPAM BOX”

---

On July 10, 2002, the CNIL announced the launch of operation “Spam Box”. This three month campaign, based on the exploitation of more than 320 000 messages received, allowed a precise picture of the phenomenon of unsolicited electronic mass e-mailings in France to be formed, the behaviour of 5 senders to be denounced to the public prosecutor, and a pedagogical “Stop Spamming!” module to be proposed on the CNIL site. The results were published on November 21, 2002. What is the situation seven months later?

---

- **The legal consequences**

Three cases (an e-mail harvester, a tourism site, a dating services site) are still in pre-trial investigation, whereas the complaints against the North American company and against the company editing “The X Top 50” have been closed without consequence, as the inquiries had not managed to identify the senders of the incriminated messages. These two decisions illustrate the difficulty of identifying senders of spams and show the limits of a legal response to the problem of spamming. The implementation of mechanisms of co-operation between the authorities charged with questions relative to spamming, both outside and inside the European Union, would certainly facilitate a more efficient handling of litigation.

- **Towards a new legal framework in matters of prospecting by e-mail**

The CNIL has given its advice on the future legal measures applicable to prospecting by electronic means in its decision on the numeric economy bill. This text, which is under discussion, lays down the principle of prior consent (“opt-in”) in the matter of direct prospecting by e-mail. The CNIL reminded us that the principle of prior consent constitutes a strong guarantee of protection of persons, a guarantee whose importance should not be lessened. It considers, furthermore, that the definition of “consent” excludes that giving it should, for example, be diluted in the accepting of the general conditions of use of a proposed service, or even coupled together with an request for reduction fee. It is with this in mind that the Commission recommends that the collection of consent should be carried out, for example, by using a box to tick.

**The problem of spamming remains more topical than ever and finding solutions are still the major stakes. Consequently, the CNIL continues its action of mobilisation against spamming :** it collaborates on the European level in the elaboration of common guidelines for the practical implementation of the new legal measures concerning electronic communications, it has participated in a forum organised by the US Federal Trade Commission, and it intervenes in the framework of the working groups which bring together the professionals of e-marketing.

Finally, the success of the “Spam Box” operation is being consecrated on the legal level by the setting up of an electronic mailbox within the CNIL which will collect the complaints concerning the non respect for the measures applicable to operations of unsolicited prospecting (a bill on confidence in the numeric economy as adopted by the National Assembly).

*See 23<sup>rd</sup> annual report, pp 45 - 55*

## THE PREVENTEL FILE : NUMEROUS COMPLAINTS IN 2002 BUT CLEAR IMPROVEMENT IN 2003

---

**The CNIL, which played the role of a “cell phone after sales service” in 2002, notes a clear improvement of the situation in 2003 : from 43 complaints in 2000, 88 in 2001, and 132 in 2002 to less than 20 complaints since February 1, 2003.**

---

In 2002, the CNIL received 132 written complaints concerning the Preventel database, the purpose of which consists in preventing unpaid bills in the telecommunications sector. This database mainly centralises information on subscribers' unpaid bills owed to mobile phone operators and to certain operators of fix telephony, which have all joined in a specific legal structure called “GIE Preventel”.

Added to these 132 formal complaints in 2002 were numerous daily telephone calls, which thus mobilised a significant number of the CNIL's collaborators.

In the majority of cases, plaintiffs contested the reality of the very debt at the origin of their registration in the Preventel file. Above all, they mentioned the complete absence of reaction of cell phone operators to their letters of complaint. As they could obtain no explanation from their operator, they contacted the CNIL “as a last resort”, thus expressing their powerlessness.

By assessing these complaints, the CNIL noted that cell phone operators, despite its recommendations, did not duly deal with the subscribers' claim contesting the debt claimed within a reasonable period of time and in a non-computerised fashion, while this contestation did not give rise to a suspension of the registration of the information in the Preventel file.

Thus, by playing the role of mediator between the plaintiffs and the cell phone operators, and in many cases by obtaining the deletion of the information relating to the plaintiff from the Preventel file, the CNIL was used – what is not its role – as the after sales service of these operators.

In January 2003 the cell phone operators members of GIE Preventel were very formally alerted on the problems raised by the Preventel file. These operators have since then made numerous commitments in order to put an end to this situation.

It is satisfactory, in June 2003, to note that these commitments have been kept.

In fact, only 17 written complaints concerning the Preventel file have been addressed to the Commission between January 1 and May 31, 2003 (in 4 months the CNIL received less complaints than it received during the sole month of January 2003). At the same time, the number of telephone calls received by the CNIL on this subject has markedly decreased: at present, it receives only a few calls a week concerning on the issue.

The CNIL considers this progress very encouraging. If this tendency was confirmed, a future assessment covering the whole year 2003 would allow the Commission to consider that the problems linked to the Preventel file have been “eradicated”.

*See 23<sup>rd</sup> annual report, p.111*

## BLACK LISTS: “BAD DEBTORS” AND “FRAUDS” ON RECORD

---

**The risk of exclusion and marginalization of individuals listed in “bad debtors” or “frauds” files, usually described as “black lists”, is at the heart of CNIL’s concerns : risk prevention must not lead to the institution of a “two-tier society” that would exclude the most disadvantaged from the guarantees offered by the law of January 6, 1978.**

---

The CNIL recently recalled the risks implied by the development of such files, and by bringing together information relative to “default of payment” or “fraudulent” behaviour, whatever the sector of activity concerned. Faced with this practice that is developing outside any specific legal framework, the CNIL wishes certain principles to be better respected:

- **“Black lists cannot be held secret”**

The necessary transparency of these files must be ensured by informing individuals about the purpose of the file and the recipients of the data as well as on the existence of the right of objection. This information must be given when the data is collected, when an incident which may give rise to registration occurs and, if need be, at the time of such registration.

- **“Individuals should not be put in the electronic stocks”**

The institution of, and access to a file must be limited to one sector. That one has not paid one’s rent does not imply that one should not be able to rent a telephone line.

- **“Conditions of registration must be strictly complied with ”**

The data controller must guarantee the relevance of the processed data : he must ensure that conditions of registration are complied with, proceed to examine any dispute and ensure that mediation and control procedures are set up.

- **“The right to oblivion must be guaranteed”**

The determination of storage periods and the existence of up-dating procedures should allow the principle of “right to oblivion” to be complied with.

- **“The security and confidentiality of the data must be ensured”**

Technical and human means must be on an equal level with existing dangers in the matter of invasion of privacy, and the risk of confusion between namesakes must be checked for.

The action by the Commission to guarantee that these principles are respected:

- A more dynamic exploitation of its central file, the “file of files”.
- Systematic audits by sector of activity.
- The elaboration of specific security rules for “blacklists”.

[See 23<sup>rd</sup> annual report, p.103](#)

## ELECTRONIC VOTING

---

**In 2002 and 2003 the CNIL was consulted on several electronic voting experiments. On these occasions it noted that the conditions of validity and security were not always combined. On each occasion it recalled its recommendations for effectively guaranteeing the confidentiality of the vote and compliance with data protection rules. A general recommendation is being prepared to meet with the expected development of electronic voting.**

---

During the presidential and legislative elections of 2002, the CNIL authorised the city of Mérignac to carry out an experimentation of electronic voting “on site”, based on smart cards and biometric identification of voters. On the other hand, it gave a negative opinion on the project of remote Internet voting of the city of Vandoeuvre-les-Nancy, upon the consideration that the system as planned did not guarantee the positive identification of the voter, the anonymity of his vote, and the control of the electoral operations (as the computer system was located in the United States).

In 2003 the CNIL accepted an experiment of Internet voting on the occasion of the election of “neighbourhood councils” in Issy-les-Moulineaux, considering the lack of a legal framework setting the conditions to respect and the principle itself of such an election. This case was the occasion to study a real experiment of Internet voting, but then with limited stakes. On the other hand, the CNIL gave a negative opinion on another experiment within the same town concerning elections to the industrial tribunal considering, in particular, that the presence on the same server of the identity of the voter and of his ballot did not ensure that the procedure effectively guaranteed the secrecy of the vote.

When examining such measures, the Commission checks that data protection rules are complied with, which implies that a certain number of technical guarantees are adopted which are indispensable to the preparation and the implementation of elections.

Thus, the secret of the ballot must be ensured by implementing procedures which prevent a link to be established between the name of the voter and his vote. Strong encryption measures must therefore be adopted. The modalities of authentication of voters must also be secure (electronic certificate, smart card for on-site voting, recorded delivery mail).

The control of electoral operations, in particular of the counting of the votes, if it is entrusted to an external contractor instead of electors themselves, also raise a question of principle.

The generation and delivery of electronic keys allowing the counting of votes to start must, therefore, be secure, as must their possession, before the close of the ballot. Finally, the computer system used must be located in a place allowing the election judge to carry out his control easily.

Electronic voting is no doubt due to fast development but it requires serious guarantees in terms of security and of vote anonymity. The CNIL should, in the near future, issue a recommendation formulating specific requirements on this point.

*See 23<sup>rd</sup> annual report, p. 79*

## E-GOVERNMENT ISSUES : MORE TOPICAL THAN EVER FOR THE CNIL

---

**After elaborating several doctrines on the development of e-government issues, in 2002 the CNIL gave a positive opinion on the implementation of several online administrative procedures through the Net Enterprises Web portal**

---

In its annual report of activity for 2001 the Commission insisted on a certain number of guidelines for e-government projects, namely : compliance with the principle of equality by the public services, recourse to sector-based personal identifiers (i.e. “to each sphere its identifier”), requirement of confidentiality, compliance with the principle of transparency. The development of e-government indeed appears to provide a remarkable opportunity for citizens to fully exercise the rights conferred by the Data Protection Act of 1978, for example to have online access to any files concerning him or her.

The positive opinions given by the CNIL in 2002 on several projects of online administrative procedures implemented in the social sector through the so-called “Net Enterprises” Web portal show that the Commission, far from having a dogmatic approach to the question, has in fact for years supported and encouraged the development of e-government projects, when they comply with the principles of personal data protection.

The current state of the law now allows employers and professional people to make their social tax declarations on the Internet. A specific service was set up in this respect, called “DUCS-I” (unified declaration of individualised contributions), which helps employers and professionals making their social tax declarations and issuing pay-slips online. The Commission’s opinion was formally requested on three projects of online administrative procedures bearing to the DUCS-I, as well as on the independent professions’ ‘common declaration of income’ and the ‘automated unified declaration of social data’ (DADS-U). In all these cases, the Commission issued a positive opinion.

The Commission also follows with particular attention the work of the Government on major e-government projects. It takes part to working groups on the project of the “monservicepublic.fr” Web portal, on the service of change of address, or on the project of daily life cards to be issued by some local authorities. The CNIL has also set up an internal working group dedicated to following the evolution of these projects.

Furthermore, upon the initiative of the CNIL, the so-called “Article 29” Working Party has realised an inventory of e-government and data protection issues in Europe, on the basis of a questionnaire to which the authorities of the European Union countries were invited to respond. The resulting working document is presented in appendix 7 of the 23<sup>rd</sup> annual report.

*See 23<sup>rd</sup> annual report, pp 16 and 153*

# SURVEILLANCE OF DISEASES SUBJECT TO OBLIGATORY NOTIFICATION: ANONYMITY NOW GUARANTEED

---

**In 2002 the CNIL authorised the system for epidemiological surveillance of diseases subject to obligatory notification, such as HIV / AIDS, implemented by the National Institute for Health Monitoring. The CNIL ensured that anonymity of personal data was complete and irreversible.**

---

This authorisation by the CNIL is the result of several years of successful work carried out in close collaboration with the National Institute for Health Monitoring (“Institut National de la Veille Sanitaire”, INVS) and in consultations with patient defence associations.

After associations of defence of patients suffering from AIDS expressed their concern as to the nominative registration of HIV positive persons, the CNIL had demanded in December 1999 that a certain number of measures, conducive to guaranteeing anonymity of the persons, be respected:

- **Anonymity** at the stage of the notifications by means of encoding of the person’s name, first name and date of birth.
- **Identification** of the person’s place of residence limited to the code of the department, and of the person’s profession to the socio-professional category only.

Furthermore, the Commission demanded that the anonymous and free testing centres (CDAG) should be excluded from the measures, as the implementation of an obligatory notification based on even the indirect identification of the person, whether encoded or not, is by definition contrary to the principle of anonymity of the CDAG.

Twenty-six diseases are concerned by the processing which the INVS submitted to the CNIL. By using hashing software one can, from the first letter of the person’s name, first name, date of birth, and gender, create a figure of anonymity in the form of a chain of sixteen characters. The irreversibility of this process prevents any link from being established between the patient’s identity and his medical data.

Although the CNIL authorised the mention of country of birth, place of residence, and current nationality of the person, it considered, on the other hand, that the mention of nationality at birth was not relevant, as such data of an administrative nature could give rise to reactions of incomprehension, or even rejection, on the part of the interested parties.

The CNIL also verified that each patient would be provided with complete and specific information.

*See 23<sup>rd</sup> annual report, p.128*

# THE NEW POPULATION CENSUS

---

**The CNIL follows with particular attention the different phases of preparation of the new population census, whose guidelines were defined by the Act of February 27, 2002. The Commission provided its opinion on the decree providing for the modalities of preparation and implementation of census surveys.**

---

Title V of the law of February 27, 2002 provides for new procedures of implementation of population census. These procedures will apply from 2004.

These new census procedures, precisely defined by article 156 of the Act, will differ according to the size of municipality. They will consist in classic census surveys in municipalities with less than 10.000 inhabitants, according to a principle of annual rotation (one municipality out of five being surveyed each year). Municipalities of 10.000 inhabitants or more will be subject to an annual procedure of population census by survey, completed by statistical data issued from administrative sources (tax files, databases registering planning permissions, social files, etc.).

An important innovation of the law is the fact that the local authorities themselves are now in charge of preparing and carrying out these household surveys.

The role of the local authorities will be important and will consist in preparing the collection of the data, ensuring recruitment, management and follow-up of the census agents, and ensuring that the collection of the data is exhaustive.

To this end, the municipalities will have to check on the field the accuracy of the addresses registered in the directory of located buildings (the so-called RIL file), which should allow the National Institute of Statistics (INSEE) to locate geographically the buildings in municipalities of 10.000 inhabitants or more. To follow the progress of the collection, they will have recourse to computer applications so as to follow, address by address, the number of questionnaires distributed, and the number of documents recovered with an indication of the date of collection. Finally, they will be entitled to process information issued from the local tax database in order to check the exhaustiveness of the collection.

**The CNIL requested that the decree should explicitly recall that this data cannot be used for other purposes than population census, so as to avoid that the data collected on this occasion is used to set up “population files” which have no legal basis in France.**

The decree was published on June 5, 2003.

The first results of this new census should be known at the end of 2008.

*See 23<sup>rd</sup> annual report, p. 146*

# IMPLEMENTATION OF THE EUROPEAN DIRECTIVE ON DATA PROTECTION OF OCTOBER 24, 1995

---

**The bill transposing the European data protection Directive is currently being examined by Parliament. The bill implies a simplification of the procedures by the “Data Protection” Act and reinforces the means of action of the CNIL.**

---

An important revision of the “Data Protection” Act, justified by the necessity to implement the Directive of October 24, 1995 on the protection of personal data is currently underway in Parliament. The bill modifying the Act of January 6, 1978 was voted by the National Assembly in its first reading on January 30, 2002 and modified by the Senate on April 1, 2003. The going back and forth between the two chambers should continue in the Autumn, although France is the only country in the European Union not to have formally transposed the Directive into National Law.

In the current state of the parliamentary work, the bill provides a simplification of the formalities with which data controllers must proceed prior to processing personal data. Numerous types of processing may be exempted from any formality or may be subject to simplified notifications only. Administrations, local authorities and other public bodies will no longer need a positive opinion by the CNIL to implement most of their applications; in most cases they will only need to notify them to the CNIL.

On the opposite, so-called “sensitive” processing of personal data, whether by a public or a private data controller, will be subject to an authorisation by the CNIL, i.e., genetic and biometric data, files of offences, “black lists”, persons in social difficulty, etc. The CNIL’s powers of on-site audit will also be confirmed and extended. Finally, the CNIL will have the power to impose financial sanctions or, in case of emergency, decide to block a processing.

Beyond this repressive aspect, which is clearly indispensable to ensuring that the law is enforced in the most serious cases, the CNIL’s modes of intervention will evolve in the sense of advice and technical expertise.

Thus, upon the initiative of Mr Alex Türk, reporter of the Law Commission, the Senate has decided that companies may avoid notification formalities by designating data protection officers who will be in continuous contact with the CNIL. The Senate has also introduced the notion of anonymisation of personal data by granting the CNIL with the mission of certifying technical processes of anonymisation. The bill also provides that the CNIL has a power of certification of products which contribute to data protection and a power of validation of professional codes of conduct.

## LAST MINUTE! THE CNIL ISSUES WARNINGS TO TWO MAJOR BANKS

---

**The CNIL has reminded two banks on the rules for registering their clients in the consumer credit national negative file (the FICP), managed by the French central bank.**

---

The CNIL noted in 2002 a tendency by certain credit institutions or banks to use the FICP as a means of pressure on their debtors, while respecting neither the provisions of the law of January 6, 1978, nor those of regulation Nr. 90-05 of the committee for bank regulations (the CRBF) relating to the FICP.

This led the CNIL to issue a warning to two banks: the “Caisse Régionale du Crédit Agricole Mutuel du Nord” and Fortis.

In both cases, the banks, which had been in litigation with their clients for several years, had only recently registered them in the FICP and for no real reason. Thus, the primary purpose of the FICP – reporting without delay cases of default of payment in order to avoid individuals becoming overindebted – had been led astray.

It should be remembered that in 1989, faced with the difficulties met by borrowers in reimbursing their credit, particularly short-term credit, the legislator adopted a measure of prevention and treatment of situations of excessive debt and, in order to respond to the lending establishments' need for information, created the FICP. This file allows banks, credit institutions, and the French Post Office financial services to have the means of additional information necessary to assessing the risks linked to granting credit to individuals.

**The FICP is therefore not a file of “undesirable clients” that financial bodies can feed as they see fit.** However, the actions noted by the CNIL show a lack of knowledge about the rules of registration in the FICP, which leads to its circumvention of its original purpose .

Such procedures, moreover, arise most often when the bank entertains conflicting relations with a client, or indeed when litigation is ongoing between them. The FICP then is used much more as a means of pressure than as a means of fighting against excessive debt of individuals.

Except for initiating a legal procedure, the client, in this case, has the CNIL as sole recourse. The CNIL's action will, in fact, allow him to see his rights preserved and his registration in the FICP deleted if it is unjustified.

*See 23rd annual report, p.105 and the guide “Protection des données personnelles et refus de crédit” (“Personal Data Protection and Credit Denial”)*