

**"PROTECTION OF PERSONAL DATA AND PRIVACY:
EDUCATION UNDER DISCUSSION"**

TUESDAY SEPTEMBER 24, 2001

CÉCILE ALVERGNAT, MEMBER OF THE CNIL

The advent of an information society and economy, with the Internet as its main infrastructure, represents one of the major phenomena of the end of the 20th century that no one can be unaware of nowadays.

Are all the consequences being truly gauged?

To allow ourselves to be fascinated by a technology that pushes back the boundaries of time and space, giving each individual a feeling of power and freedom, would be to forget that the Internet is questioning our values just as deeply : the values of our democracies.

More than any other technology, the Internet is blurring the boundaries between our professional career and our personal activities, the boundaries between public life and private life.

We can hardly even glimpse the potential threat posed by it: a personalisation tool can also become a tool for "merchandisation" of people; and a tool for freedom and expression of our individuality can become a tool for control without people knowing. Taking stock of these phenomena means making them visible from the viewpoint of the values and principles that we have adopted, the freedoms that we set out to respect, because these values are fundamental and widely shared, be it in the Universal Declaration of Human Rights of December 10, 1948 or the Charter of Fundamental Rights of the European Union of December 2000.

Reasserted each time, these values should inspire our outlook on technology.

Are we taking full control?

Citizens now live alongside these technologies without having had the time to adapt to them.

The new generation is of course launching itself headlong into them and it controls perfectly the techniques without really being aware of what is at stake. But what about the other generations that board the train whilst it is moving?

It is the entire stake of the public discussion and the necessary education that is fuelling it:

- Ensure that individuals are able to adapt to these technologies with full knowledge of the facts;
- Ensure that these technologies do not develop without their knowledge, and that citizens are not faced with a "fait accompli";
- Be transparent so as to allow citizens to be in a position to choose and avoid their only solution being that of being forced into rejection after the event;

This is the context surrounding the CNIL, whose tasks are, at the same time, to fuel public and social debate and to make the law more accessible.

Fuel public and social debate

To increase awareness, adopting an educational role, involves first of all **discussing, informing and making the general public understand**. In drawing up a technical and legal inventory, the CNIL is in a position to highlight possible inadequacies in existing law on account of technological developments and new customs arising from this which, if we are not on our guard, might well threaten our values.

In anticipation of new, particularly heavy-handed regulations to be implemented, above all when this involves a law, the CNIL is endeavouring to spotlight paths towards solutions, practical elements in the form of recommendations, which the players will, in general, be all the more anxious to follow if the solutions have been developed in consultation with them.

On a topic such as the Internet, the CNIL first of all attempted to spell out the general principles for data protection applicable to the Internet in the most sensitive areas: e-commerce, e-mailing, e-health, cyber-surveillance of employees within the company or even protection of minors. A fascinating new, but highly complex, avenue is opening up, namely, e-administration.

As early as 1998, to increase awareness among citizens of the possible consequences of Internet use with regard to protection of data and privacy, the CNIL created on its site a heading entitled **“Your tracks: discover how you are being trailed on the Internet”**. It offers Internet users a simulation that enables them to discover what the stakes are when these techniques are used. It advises them on the attitude to adopt: be realistic, demand implementation of the law and ensure rights are respected.

From among the topics dealt with during the course of 2001, let us now focus on two areas, illustrating the methodology adopted by the CNIL.

E-health

In this field, the method was that of checking specialised companies *in situ*, supplemented by an online audit of 59 health sites. The aim was to assess implementation of the law on data processing and freedom (informing Internet users of their rights, security systems, registration, etc.) and thus obtain, at a given moment, a snapshot of the state of data protection in this field.

The results of this study were only moderately satisfactory. The Commission then set out, as it had done previously with regard to e-commerce, to draw the attention of site managers to practical recommendations for fulfilling their obligations and informing Internet users, in concrete terms, of their rights.

The Commission thus wished to reaffirm that health data, being of a directly or indirectly nominative nature, whether they had been communicated to the site by the Internet user and/or by a health professional, should be subject to special protection, in compliance with medical secrecy, and should not be able to be exploited for commercial purposes or transmitted to anyone at all for commercial canvassing. Concerning the nominative use of

traffic data and their possible transfer to third parties, the Commission felt that such operations should be subject to express consent from the person concerned, obtained through a box to be ticked.

Following these works, a working party, in which the CNIL is participating, was set up on the initiative of the French Ministry of Health and the French National Council of Doctors with a view to drawing up an ethics charter likely to result, in the future, in a move towards certification of “e-health” sites, as may happen in a number of countries. (sheet 1)

Internet and the young

In this case, the Commission conducted a preliminary overall study, following which it went through a process of consultation. The aims of this method of consultation were twofold: the first was, of course, to enable associations to express their point of view and their concerns, though very often we noticed that a number of these associations had not truly discussed data protection or that the discussion that they had conducted did not focus on these latter problems. In this case, the aim of the consultation was essentially to gather observations rather than encourage discussion on a topic that had not been dealt with before.

In its report, the CNIL first of all identified:

- the situation in Europe and in the world (various initiatives taken by the European Commission, the Member States, US initiatives and their legislation)
- technical solutions aimed at making protection of minors effective,
- the legal environment in France : the concept of minority
- a panel of sites intended for young people, on which it conducted an online audit
- the players involved, so as to draw up a list of the main structures representing them: professionals from business and distance selling, desktop publishing, and family and consumer associations and institution players, such as the French Child Protection Agency or the ministries concerned (Family and Education).

The recommendations made in this report were then sent to all the individuals and bodies that were consulted so that they could pass them on.

Attention can thus be drawn to the following recommendations:

- In chat rooms or forums dedicated to minors, it should be clearly displayed, on entering the site, that they should not disclose their address, nor that of their parents, or any other specific identification information;
- When collecting personal information from minors:
 - . The rule of a processing “purpose” should lead sites aimed at minors to only collect information that is strictly necessary for the purpose.
 - . Any collection of information from minors concerning the family circle, the way of life of the parents and their socio-professional status should be regarded as excessive and underhand.
 - . It is prohibited to record data relating to racial origins or political, philosophical or religious opinions or membership of unions, or the moral standards of individuals, except with the express consent of these latter (article 31 of the law of 6/1/1978). Collection of such information from children should be considered as prohibited,

unless the party responsible for the site is able to provide evidence that the parents have expressly consented to this.

Under no circumstances should the incorporation of a game or lottery intended for minors lead to transferring to third parties the information collected in this way, if the party responsible for the site is not able to prove that the parents have expressly consented to this.

In the case of using a photograph of a child on the Internet, whatever the medium employed, use and publication of a photograph of a child may only be envisaged with the child's consent and the express authorisation of the child's parents or legal guardian.

Under no circumstances may a site which a child has not connected to beforehand send information of any kind whatsoever to the child.

In respect of contacts which a site may suggest to a minor to enter into, through a letter of information, only the e-mail address and age of the minor should be collected, to the exclusion of any other information that might be considered as not complying with the stated purpose.

As it is not designed exclusively for professionals, and as it may also be directed at young people themselves, the CNIL has set up a "junior space" within its site, which is intended to shower children with advice on surfing with complete peace of mind.

They can thus:

- access the heading "Your tracks", which is appropriate for minors,
- find out their rights,
- take part in a question and answer game,
- send an e-card to a friend.

E-cards and an information pack relating to the "junior site" are widely circulated by the Commission. The CNIL encourages the development of links with its site, which was done by the Ministry of Education, the French Child Protection Agency and the French Embassy in Washington.

As the report recommended, and as has been established in other countries, it is envisaged that a national information day could be organised in primary schools, secondary schools and colleges by the Ministry of Education in collaboration with the ministry with special responsibility for the family and children, the inter-ministerial Commission for the Family and various associations involved. On this occasion, an information campaign was envisaged. (sheet 2)

Lastly, in the same way, following studies on cyber-surveillance of employees within the company and on procedures of "seal of approval" and "certification" of e-commerce sites, the CNIL has published its recommendations. (sheet 3 and 4)

Make the law more accessible: A law in motion

As a regulatory body, the CNIL is able to bring fast responses that are appropriate to developments in technology and its uses.

The CNIL is anxious to enforce a pragmatic and reactive approach that makes it possible to increase awareness both among professionals, the general public and institutional players.

The results of the assessment of data protection conducted on 100 e-commerce sites revealed positive aspects, above all when the sites had been registered with the CNIL, as well as some shortcomings. This situation led the Commission to contact the natural relays, professional organisations with projects for “seals of approval” and “certification” of Internet sites. Recommendations on the procedures to be implemented were drawn up at the end of 2000 and systematically forwarded to the various parties. (sheet 4)

A number of examples of private initiatives of French origin are given below:

- [L@belsite](#), launched within the context of the French National Business Council and the International E-commerce Institute, which was set up and developed by the FED (Fédération des entreprises du commerce et de la distribution) and the FEVAD (Fédération des entreprises de vente à distance) which sets out to adopt a European dimension.
- Webcert, launched by the AFAQ (Association française pour l'assurance de la qualité), a non-profit making independent body specialising in certification, which received the accreditation of the COFRAC (Comité Français d'Accréditation).
- Other initiatives are coming into being, such as the French subsidiary of the Bureau Veritas Group, which is accredited in France for issuing certificates of quality for products and services, as well as more directly European initiatives such as the Trust Info-ChamberSign, which groups together the chambers of commerce of the Member States, and Globalsign with an international vocation of Belgian origin.

Although no provision of the law of the 6th January 1978 grants the CNIL the authority to award any certificate, seal or label attesting conformity to an existing law on protection of personal data and privacy, the commission, which has a duty to advise, remains closely associated with the work carried out by these bodies.

This same method is used when a matter is referred to the commission to examine and comment on **draft professional codes of ethics**. For example, as early as 1993, the professionals in direct marketing and distance selling (UFMD) adopted a professional code of ethics in close collaboration with the CNIL.

In 1997, the two main operators in mega databases also submitted a professional code of ethics to the Commission.

Companies in commerce and distribution (FCD) did the same in 1999.

Lastly, this year the Commission gave its decision on the professional code of ethics of the French professional association of customer relations centres (AFRC). (sheet 5)

I shall conclude this talk by simply stating my deep conviction that it is on account of the force and quality of this ongoing dialogue, nourished by the diversity of the points of view of

lawyers, companies, government and citizens, that the necessary maturity can develop, allowing the emergence of appropriate responses to technological developments and thereby ensure real protection of our personal data and our privacy.