

FRA

Thematic Legal Study on assessment of
data protection measures and relevant
institutions
France

Elisabeth Lambert Abdelgawad

Strasbourg, France
February 2009

DISCLAIMER: This thematic legal study was commissioned as background material for the comparative report on *Data protection in the European Union: the role of National Data Protection Authorities* by the European Union Agency for Fundamental Rights (FRA). It was prepared under contract by the FRA's research network FRALEX. The views expressed in this thematic legal study do not necessarily reflect the views or the official position of the FRA. This study is made publicly available for information purposes only and do not constitute legal advice or legal opinion.

Contents

Executive summary	3
1. Overview.....	5
1.1. Normative framework	5
1.2. Current debates	6
2. Data Protection Authority	7
2.1. Remit and Powers.....	7
2.2. Budget and Independence.....	14
3. Compliance.....	17
4. Sanctions, Compensation and Legal Consequences	18
5. Rights Awareness.....	22
6. Analysis of deficiencies	24
7. Good practices	26
Annexes	28

Executive summary

- [1]. In France, the protection of personal data is considered to be inextricably linked to the right to privacy; however, the right to this specific protection is not mentioned in the Constitution. The protection of personal information is regulated by the CNIL (French Data Protection Authority). Founded by a 1978 law, the CNIL was the first independent administrative authority. Since 2004, with the adoption of the French law for the application of the European directive of 24.10.1995, this regulatory body has acquired more power (most importantly, through the right to impose sanctions, but also because of the requirement for a CNIL authorisation for the processing of information deemed sensitive because of its use or because of the nature of the data being processed (Art. 25 of the law), and through the insertion of Correspondents of data-processing and freedoms in the workplace. Very few sanctions have been imposed, for two reasons: the slow increase in importance of this new power given to the CNIL, requiring it to take all necessary measures in conformity with the right to a fair trial. In 85 per cent of cases, the entity conforms to the order, which is representative of the efficiency of the sanctions procedure. Awareness campaigns seem to have only recently paid off. Many initiatives have been put in place, although the need for further efforts remains obvious.
- [2]. Today, various actors agree on these deficiencies: the lack of personnel and budgetary means to meet the demands of the important increase in the CNIL's activities, which puts France in a bad position with regard to other member states of the European Union. In 1978, France prided itself on being one of the pioneers in the protection of personal data. Campaigns to increase awareness about the role of the CNIL, especially within public administrations, also seem to be limited. Also, state databases are subjected to recommendations, and sometimes authorisations, when they fall into the category of article 25, as well as to watch and sanction procedures (which are occasionally adjusted), as well as to an indirect right of access, and are given a special status. It seems that an overhaul of the 2004 law is necessary on many levels, for example to further relax the process of preliminary statements. A group within the CNIL is currently studying the possible revision of the law Data Processing, Data Files and Individual Liberties.¹
- [3]. Current Parliamentary and public debates focus on the lack of budgetary means and the under-representation of the opposition within the CNIL², as well as the

¹ CNIL, *Annual Report 2007*, p.75. The conclusions have not yet been finalized. The only specific information included in the report is the following : “the declaration formalities are still poorly understood as they are too complex; the reality of international transmission of data is not completely covered in the law; information on individuals' rights should be more specific; the operational system of the institution must be modified in order to make its actions more efficient and rapid....”

² Which was partially remedied by the nomination of a Senator from the opposition in December 2008.

need to adapt the processing of data for security reasons. Above all, the debates in recent months have centered on the establishment or the revision of certain state databases. Besides the data storage system EDVIGE, which caused public uproar during a large part of 2008, due to a publication acquired by the CNIL, on 10.12.2008, a report entitled '*Improve the implementation of data processing to better respect liberties*'³ was published.

³ Groupe de contrôle des fichiers de police et de gendarmerie (2008), '*Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés*', Report submitted to the Minister of Home Affairs, Overseas, and Regional Authorities.

1. Overview

1.1. Normative framework

- [4]. The protection of personal data is indirectly protected by the French Constitution through the second article of the Human Rights Bill of 1789, which guarantees the right to the protection of privacy. In spite of certain initiatives, the constitutional reform of 2008 did not bring about the inclusion of the right to protection of personal data in the Constitution⁴. However, the Constitutional Council has referred to the law on *Data processing, Data Files and Individual Liberties* as the ‘protector of individual freedoms’⁵. Also, this law is given the special status of a law for the protection of the constitutional value of individual freedom. This value is considered to be a fundamental constitutional principle⁶. The Constitutional Council has had the occasion to issue decisions concerning the constitutionality of certain laws on the protection of data. However, it has always considered that it is the Legislature’s role to reconcile existing regulations, and so it has never declared any of these laws unconstitutional – something which has raised criticism.
- [5]. With regard to international standards, independently of the UN Guidelines concerning computerized data files (14.12.1990), as well as the guidelines provided by the OSCE on the security of information and the protection of privacy, France is legally bound by Article 17 of the ICCPR, to which it adhered without reservation, by the Schengen Accords, and Convention 108/81 of the Council of Europe for the protection of persons with regard to the automated processing of personal data as well as its Additional Protocol concerning competent authorities and the cross-border transmission of data.
- [6]. The principal piece of legislation is the law on *Data processing, Data Files and Individual Liberties* of 1978⁷, which has since been modified numerous times, mostly because of the obligation to comply with Council Directive 95/46 (24.10.1995), through law 2004-801 (06.08.2004). An important change consisted in the disappearance of distinctions between the public and private sectors, which was replaced by a distinction based on the level of sensitivity of information.

⁴ J.M. Pastor (2008), *La CNIL veut inscrire la protection des données dans la Constitution* », in : *Actualité Juridique Droit Administratif*, p.964.

⁵ France/Conseil Constitutionnel/92-316 (20.01.1993).

⁶ France/Conseil Constitutionnel/76-75 (12.01.1977).

⁷ France/Loi 78-17 (06.01.1978).

- [7]. The competent institution in charge of these matters in France is the CNIL (French Data Protection Authority). Founded by a 1978 law, the CNIL was the first independent administrative authority (<http://www.cnil.fr>).

1.2. Current debates

- [8]. Current debates on the protection of data concerning topics other than the CNIL's lack of budgetary means tend to focus more on specific issues than on the general deficiencies in the system. While some authors argue that not one single Parliamentary study or debate on the subject in thirty years⁸ can be mentioned, the establishment of a Parliamentary mission, which was established for police databases at the National Assembly as an extension to Edvige⁹, – an intelligence database put in place by the Minister of the Interior in the process of reform of French intelligence services- must be noted. The relationship between the protection of data, and public security demands, has also been discussed,¹⁰ as well as the evolution of technology.¹¹

⁸ J. Frayssinet (2008), 'Dossier spécial, Les trente ans de la loi "Informatique et libertés"', in : *Revue Lamy Droit de l'Immatériel*, n°34.

⁹ EDVIGE: Exploitation documentaire et valorisation de l'information générale.

¹⁰ Informational Report submitted by the Delegation of the *Assemblée nationale* to the European Union on the exchange of data and the protection of personal data in joint police and criminal control operations, presented by M. Christian Philip, Deputy, on 13.12.2007. See also the bill HADOPI on the protection of copyright.

¹¹ Report from the Parliamentary office on scientific and technological choices, on the evolution of the micro/nanoelectronic sectors, by M. Claude Saunier, Senator, dated 25.06.2008.

2. Data Protection Authority

- [9]. The CNIL is an independent administrative authority. The employees of the CNIL are public sector contract employees. Its President (Alex Türk) has Ministerial status and is selected by (and from among) the Members of CNIL, who are themselves nominated by the government, Parliament and the judiciary. More precisely, the CNIL has a pluralistic college composed of 17 personalities: four Members of Parliament (two Deputies, two Senators), two Members of the Economic and Social Council, six representatives of the highest French courts (two Councilors from the Conseil d'Etat, the French Administrative Supreme Court, two Councilors from the Cour de Cassation, the French Supreme Judicial Court, and two Councillors from the Cour des Comptes, the French Revenue Court); five qualified personalities, one being appointed by the President of the National Assembly, another by the President of the Senate, and the other three by the Council of Ministers. The term of office of its members is of five years or for duration equal to the elective term of office of the Members of Parliament. The President of the CNIL freely recruits his collaborators (article 10 of the Act). It should be noted that Jurists represent the majority of employees within Operational Services of the CNIL. The composition of the Commission was set forth by the legislature, so as to guarantee independence and representative diversity among members of the Commission.

2.1. Remit and Powers

- [10]. The remit of the CNIL is detailed in articles 2 and 5 of the Act of 1978. According to article 2, the Act of 1978 applies to automatic processing of personal data as well as non-automatic processing of personal data that is or may be contained in a personal data filing system, with the exception of processing carried out for the exercise of exclusively private activities, where the data controller meets the conditions provided for in Article 5 (*subject to national law*). Following article 5, the data controller has to be established on French territory. Should the data controller be established in any other Member State of the European Community, the CNIL is competent if the data controller uses means of processing located on French territory, with the exception of processing used only for the purposes of transit through this territory or that of any other member State of the European Community.
- [11]. According to French law, Personal data means any information relating to a natural person who is or can be identified, directly or indirectly by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller

or any other person uses or may have access to should be taken into consideration (article 2 of the Act of 1978).

- [12]. The powers of the CNIL are diverse. First, the CNIL informs the persons concerned of their rights and obligations. Second, it proposes to the government all necessary legislative or regulatory measures for adapting the protection of rights and liberties to evolving technologies. The opinion of the CNIL must be sought before any bill may be sent to Parliament calling for the automated processing of personal data. The CNIL makes sure that the terms governing the right to access data do not hinder the free exercise of this right. The CNIL responds to all requests for advice and consultation it receives. The CNIL makes a count of the computer files; authorisation is required for the processing of 'sensitive' data. It records the implementation of all computer files and makes available to the public all the processing of which it has been notified with an indication of their purpose, of the place where the right of access is implemented, and of the categories of people who receive the information (more than 800,000 notifications to date). The CNIL possesses special powers to have the law enforced. The CNIL can, on its own initiative or following a complaint by an individual, carry out audits on the spot concerning any database. It therefore adopts recommendations for a correct implementation of the law; 28 recommendations have been enacted to date on the most varied subjects. In case of offences, the CNIL may issue warnings to the persons responsible for the database or inform the Public Prosecutor of any offences it has knowledge of or makes use of its new power to sanction, according to the reform of 2004. It promotes the adoption of professional rules of good conduct in various professional sectors (direct marketing, call centres, mass marketing). It also has a mission of expertise and technological monitoring: the CNIL keeps itself informed of the evolution of technical processes; it draws up reports which are submitted to public consultation (databases for combating fraud in matters of consumer credit, advertising via email, biometric recognition technologies, the Internet and minors, cyber-surveillance in the workplace, etc.).
- [13]. The main concern is to appreciate whether French law is conform to the European Directive. The law of 1978 goes further Article 28.2 of the directive, specifying that the CNIL must be consulted on any bill or decree related to the protection of individuals, with regard to the automated processing of data (Art. 11.4°a), and that it must propose legislative and regulatory measures to the government so that the protection of freedoms and privacy may be adapted to the evolution of data-processing techniques.¹² French legislation complies with Paragraph 3 of the directive, as the CNIL has different investigative powers. Its role is to see that the processing of personal data be conducted in compliance with the dispositions of the law; it authorises processing described under Article

¹² In 2007, the CNIL provided six recommendations on bills and decrees (see p. 83 of the *Annual Report 2007*);

25,¹³ and gives its opinion on processing related to national security and criminal offences. It also receives declarations about the other types of processing carried out.¹⁴ It may assign one or more of its members or agents to conduct checks on all types of data processing, and to obtain copies of all documents or support information useful to its mission, according to conditions described under Article 44 (on-site control) - this power is similar to that described in the directive. The CNIL also has the power of intervention according to Article 25 of the law of 1978, an authorisation must be requested from the CNIL to conduct the processing of data considered 'sensitive' because of the its purpose or because of the nature of the data being processed (biometric data, data describing individuals' social difficulties, data containing individuals' national registration number or social security numbers, etc.; in this respect the law goes even further than the demands of the directive. For processing described under Articles 26¹⁵ and 27¹⁶ of the law, only an opinion from the CNIL is published. According to Article 11(g), it may, under the conditions set forth under Chapter VII (Sanctions), decide to impose on the person responsible for data processing one of the measures described under Article 45 (Sanctions and Urgent Measures). The CNIL does not have the power to sue in cases of violation of national dispositions for the application of the directive, but it does have the power to bring the violations to the attention of judicial authorities. According to Article 40 of the Code of Criminal Procedure, the CNIL must also, without delay, inform the Public Prosecutor of the violations, and it may present its own observations during the criminal proceedings, under the conditions set forth by Article 52 (observations submitted or presented by the President or by his/her representative). Contested CNIL decisions may be appealed before the Administrative Court. With regard to cases brought before the CNIL by plaintiffs he CNIL follows the procedure described under paragraph 4 of Article 28 of the directive as it receives demands, petitions and complaints related to the processing of personal data, and must inform plaintiffs of its decision. It also responds to requests for its opinion from authorities, as well as from courts, and advises individuals and organisations on the automated processing of personal data.

- [14]. While the powers granted to the CNIL correspond to those established by the European directive, certain points deserve to be commented upon. The databases established by the State fall under authorisations decreed by the appropriate Minister(s). The recommendation of the CNIL is required for their creation. However, this recommendation is only of advisory nature, and the government is not required to comply or adopt the modifications suggested,

13 Data containing information of the following nature: political, philosophical..., related to health or sex life, genetic, criminal, the national registration number (NIR); social difficulties, biometrics, etc.

14 In practice, the number of controls conducted has increased from 12 in 2003 to 218 in 2008. The punishment for interfering with the CNIL's work has already been applied by courts.

15 Security or criminal-related processing.

16 Information from the National Registry, biometrics,

whereas, before, the government was not able to proceed without a decree with the assent of the Council of State. This loophole has been pointed out by several members of Parliament with diverse political affiliations.¹⁷ However, it should be mentioned that in the past, the CNIL had never used its power to issue recommendations of non-compliance under Article 31 of the old law on the processing of sensitive information. The system of requiring the authorisation of the CNIL may also apply to computerised files created by the State when Articles 26 and 27 do not apply. Secondly, it may seem problematic that some of these databases are exempted, by Council of State decree, from the publication of the decree authorising their establishment. During the introduction of the law, the Ministry of Justice at the time, Marylise Lebranchu, specified that the opinion of the CNIL would be published at the same time as the decree authorising sovereign processing ‘so that the CNIL’s observations and reservations may be known to all’.¹⁸ However, this is not always the case. It was already this way under the law of 1978, even before its revision in 2004 (Article 20). Therefore, the police database ‘Edvige’ was created on 27.06.2008, by decree, and should have benefited from this system to avoid submission to the control of the CNIL. The CNIL eventually pushed through its publication so that a public debate could be held¹⁹ and since then, indirect access applies to this database. A new French database, called ‘CRISTINA’ (Centralisation of intelligence services to guarantee security of the territory and national interests), which was the subject of a CNIL deliberation at the same time as Edvige, has been classified as a defence secret. Therefore, the decree which authorised its creation did not appear in the Official Journal and it will not be submitted to control by the CNIL.²⁰

- [15]. It is also important to detail the powers the CNIL can exercise on its own initiative, the power to regulate and monitor, and the power to sanction. The CNIL uses its power to make sure that the law is respected, in an a priori fashion, (through a preliminary overview), and a posteriori (through visits to companies and entities, sometimes, but not necessarily, following a complaint). The CNIL can impose sanctions in different ways (warnings, formal notices, injunctions, and pecuniary sanctions). Half of the audits conducted by the CNIL are part of the annual program adopted each year during the Commissions’ plenary sitting, and result from complaints, the Commissions’ own initiatives, or previously decided sanction.

¹⁷ See debates held at the time of the modification of the law of 1978 : See comments of Martin Lalande, UMP Deputy, stating that the ‘text is proof of a certain slackening – which is a euphemism – in the control over certain public databases’ (Parliamentary Debates, Regular Sitting, 2001-2002 – 55th day of session, 127^{ème} session), or Jean-Pierre Michel’s comments, PS Deputy, who ‘insisted on the danger of giving up the distinction between databases created in the public sector and those from the private sector’ (Summary of 18th commission on constitutional law, legislation and the national administration, session held on January 9, 2002).

¹⁸ Parliamentary Debates, Regular Sitting, 2001-2002 – 55th day of session, 127th session.

¹⁹ CNIL website, announcement “Opinion on the database Edvige”, www.cnil.fr/index.php?id=2488 (19.11.2008).

²⁰ *Nouvel Observateur*, 10.09.2008: www.tempsreel.nouvelobs.com (20.11.2008).

- [16]. The decision to conduct an audit is made by the President of the CNIL, upon recommendation by Audit Services. The decision of whether or not to alert the Data-Processing Manager in the entity where the audit will be carried out is made with consideration to the mission's specific nature. The manager of the entity where the audit on the processing of data will be conducted is notified of the President's decision at the beginning of the audit. The District Attorney is informed of the date, time, and purpose of the audit before it begins. If the manager of the entity being audited objects, the operation cannot take place without the authorisation of the President of the district court with jurisdiction over the entity in question, or by a judge who has been specifically delegated by the President. The judge is petitioned by the President of the Commission. The judge's ruling comes in the form of a reasoned order. The judge who authorises the visit also oversees the audit of the entity and may personally be present during the intervention. At any moment, he/she may decide to stop or suspend the operation.
- [17]. It seems that the CNIL only rarely uses its power of initiative. Instead, it tends to prefer to function according to the following: 'any person may contact the District Attorney via mail to file a complaint with the CNIL requesting that an audit be conducted, warnings be made, a solution be reached between parties, or to request that the CNIL reports those responsible for violations to the Public Prosecutor'.²¹ However, the proactive nature of the CNIL's work goes further than its capacity to regulate and sanction, as the Commission may make proposals, and it is attentive to the needs of citizens and data-processing managers.²²
- [18]. Audit procedures are governed by Articles 11-2°- f and 44 of the law on Data Processing, Data Files and Individual Liberties, and by Articles 61-69 of the decree dated 20.10.2005, modified by the decree dated 25.03.2007.
- [19]. The agents responsible for carrying out audits are governed by Article 19 of the law. Upon request by the President of the Commission, they may, in certain cases, be assisted by designated experts. Certain audits require special authorisations, as set forth by the law (computerised files covered under Article 26 of the law of 1978²³ or secrecy-defence). Once the decision to conduct an audit has been made in the proper form, the CNIL can begin operations. The principal objective of an audit is to collect a maximum amount of information (technical and legal elements) to allow the CNIL to understand the conditions surrounding the automated processing of personal data. The CNIL's focus is occasionally specific (security, personal data, data processing methods, etc.). The CNIL may request all of the documents necessary to complete its mission –

²¹ M.-P. Fenoll-Trousseau, 'Protection des données à caractère personnel. Circulation de l'information', in: *Jurisclasseur Communication*, n°4736, §64.

²² For instance the CNIL decided to initiate a study on vidéosurveillance; consequently it requested the government and Parliament to amend the law.

²³ Data processing on behalf of the State or processing authorised by decree by the Council of State.

whatever they may be – and produce copies. The CNIL may also have access to all computer programmes and data. Article 51 of the law sets forth that interference with the work of the CNIL agents or members is punishable by one year of prison and a € 15,000 fine. The CNIL may have access to all places between 6 a.m. and 9 p.m. where the processing of personal data is conducted. There are, however, some obstacles. The CNIL can be refused access to information on the basis of the obligation of professional secrecy, and certain people argue that the language in Article 21(3) is not precise enough.²⁴

- [20]. Therefore, the CNIL has the power to decide if an action interferes with its work, and may bring its case before a court of law. The threat of punishment for interference with the work of the CNIL has led many to refrain from claiming the obligation of professional secrecy during audits. Only processing related to national security is exempted pursuant to the Supreme Administrative Court decree on the publication of laws (Article 26, III, revised). On-site checks may be also exempted under the terms of this same decree; this was interpreted by some as a ‘legal regression’.²⁵ With regard to sanctions, it is necessary to underline that although 60 per cent of audits show no irregularity requiring a sanction, the remaining 40 per cent have led to sanction proceedings, which means a formal notice from the CNIL. In 85 per cent of cases, the organisations comply with the formal notice, which leads to the termination of proceedings; sanctions are only imposed in 15 per cent of cases. Violations to individuals’ rights and freedoms are most often the result of a malfunction or ignorance of the law and not intentional
- [21]. In twenty-five years, only slightly more than 300 audits were conducted. A reversal in this trend should be highlighted. The CNIL has increased the importance of Regulatory Services and has considerably added to its workforce, and its number of on-site missions. In 2007, the CNIL conducted 164 audits, which represents an increase of 21 per cent in comparison with 2006; 40 per cent resulted from complaints from individuals. In 2008, 218 audits were conducted, which represents almost as many as in the last 25 years.
- [22]. In four different CNIL documents (a report from 2002, two opinions from 2003 and 2007, and a recommendation from 2006), direct references are made to the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data. In the 2002 report,²⁶ the CNIL specifies that the report is provided to the Article 29 Working Party, explicitly recognising the importance of the Working Party. In the 2003²⁷ Opinion, reference is made to the two Opinions issued by the Article 29 Working Party; moreover, the content

²⁴ F. Fourets (2005/6), ‘La protection des données, ou le symbole d’une démocratie nouvelle. Le contrôle de la CNIL’, *Informations sociales*, n°126, pp. 94-103.

²⁵ J. Frayssinet (2005), ‘La loi relative à l’informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004: continuité et/ou rupture?’, *RLDI*, vol.9, n°267.

²⁶ France/CNIL/Deliberation 02-004 (05.02.2002).

²⁷ France/CNIL/Deliberation 03-054 (27.11.2003).

of these Opinions is also referred to. In the 2007 Opinion,²⁸ an Opinion issued by the Working Party (Opinion 3/2005) is cited in the preamble by the CNIL, but it does not seem to influence the CNIL's position. In a 2006²⁹ recommendation, it is cited in the preamble; it mentions two opinions issued by the Article 29 Working Party (the Opinion dated 09.13.2001, and the Opinion dated 25.11.2005). The content of these opinions is used by the CNIL in its reasoning and seems to have influenced its decision, in the form of a CNIL recommendation. It is therefore possible to notice a limited influence of the Article 29 Working Party's opinions. The writing of jurists reveals that they do not think that the decisions of the Article 29 Working Party have much authority; however they do mention its work regularly.³⁰ Its influence may work in the opposite way.³¹ In the beginning of 2008, the G29 conducted a self-evaluation of documents produced by the group to be used as an instrument for the standardisation of national practices.³²

- [23]. The CNIL is 'consulted on every bill and decree related to the protection of individuals with regard to the automated processing of data' (Art. 11), (but not on 'non-governmental bills' from members of Parliament³³), and more generally, on the compliance with the law of professional rules, products and procedures designed to protect personal data, and to keep information anonymous. The CNIL possesses the power of initiative to propose legislative and regulatory measures to the government for the modification of the protection of freedoms to fit the evolution of computer processing techniques. The CNIL gives its opinion on the data processing techniques in place at the State level, which is related to national security, defence and public security, and which can be used for measures of prevention, research, and ascertainment, tracking of criminal offences, and criminal sentencing, or for safety measures. It also gives its opinion on the processing of personal data for the account of the

²⁸ France/CNIL/Deliberation 2007-368 (11.12.2007).

²⁹ France/CNIL/Deliberation 2006-066 (16.03.2006).

³⁰ L. Dauxerre (2008), 'Le corps, carte d'identité du salarié', *La Semaine Juridique Sociale* n° 46, 1578. M. Melin (2007), 'Salarié, employeur et données informatiques: brefs regards croisés sur une pièce à succès', *Revue Lamy Droit de l'Immatériel*, n°23-49, p. 190.

³¹ 'The CNIL's position was adopted by the European Community, and specifically by the group of European authorities dedicated to the protection of personal data, called "The Article 29 Working Party", which adopted a recommendation on 01.02.2006, referring heavily to an orientation document published by the CNIL in November 2005.' A. Mole (2007), 'Le rapport sur les alertes professionnelles est-il Cnil-compatible? Quelles conséquences pour les entreprises?', *Semaine Sociale LAMY*, n°1310 Supplemental Chapter II, p. 8. (translation by the author).

³² The study proved the importance of more precise recommendations, which paid off in the opinion issued on the conservation time of searches by search engines, in April 2008. This self-evaluation study therefore helped to reorient the G29's work to make the group more efficient and useful both to authorities in the protection of data and to data-processing managers. Another illustration is provided by the study conducted for the BCR (internal rules of procedure) in which the framework approved by the G29 is used by the CNIL to provide information to each group.

³³ But the members of Parliament may call upon it for its opinion, which was done for the first time at the end of 2006-beginning 2007: M.-A. Ledieu (2007), 'La CNIL est saisie pour la première fois sur une initiative parlementaire', *Communication Commerce électronique* n°1.

State (for a legal person governed by public or private law, providing a public service) on data containing the registration numbers of individuals from the National Directory of natural persons, and the processing of personal data executed for the account of the State consisting of biometric data necessary to confirm identity or for identification checks. Pursuant to Article 27.4, there is an obligation for any teleservice with access to individuals' personal identification information to submit information to the CNIL. In 2006, the CNIL issued nine Opinions on bills and decrees and two recommendations; in 2007, it issued six opinions on bills and decrees. Previously, the CNIL issued authorisations, which have now given way to Reasoned Opinions, which are published in the Official Journal along with decrees. The CNIL is not always consulted when a database is created by the Legislature, and as the law is more and more detailed, the decree therefore has a more limited scope; as the opinion that the CNIL issues may only be based on what is set forth by that part of the law, the opinion is also limited³⁴. This is problematic.

2.2. Budget and Independence

- [24]. The budget of the Commission is charged to the State budget. More precisely, the CNIL's funds are linked to the budget of the Department of Justice and are composed of personnel and operational credits. The initial Finance Act of 2008 provided for the allocation of € 11.33 million to this administrative authority, of which € 7.17 million were dedicated to personnel-related costs and € 4.16 million dedicated to operational costs. Between 2003 and 2008, the credits registered on the CNIL's budget went up by 74 per cent, including an increase of nearly 98 per cent for expenses related to operations. For the year 2008, there was an increase of 14 per cent, which represents three times the increase of credits for the entire Department of Justice. With the addition of 15 new job openings accounted for in the 2008 budget, the CNIL will have 120 employment positions at the end of 2008 and 131 in 2009.³⁵
- [25]. The CNIL will not be able to continue to assume its role without an increase in its budget. The same remark can be made concerning the CNIL's personnel. There is a ration of 1.6 CNIL agents to every one million inhabitants, which puts France in last place behind the rest of the member countries of the European Union.³⁶ The growth of the CNIL's activity has been greater than initially imagined at the time of the adoption of the 2004 law. Its new regulatory missions, the sanctions, the coordination of networks of Correspondents of

³⁴ F. Gicquel (2007), « *La CNIL exerce-t-elle un contrôle des fichiers de police suffisant ?* », in : *Actualité Juridique Pénal*, p.69.

³⁵ The Ministerial Committee's projections are annexed to the draft finance law for 2009 (*direction de l'action du gouvernement*), p.116.

³⁶ CNIL, *Annual Activity Report 2007*, p.95.

Data-Processing and Freedoms, and public awareness, as well as its support operations associated with the development of CNIL ‘activities-jobs’ require sufficient budgetary and human resources.

- [26]. In light of this, the draft finance budget for 2009 allocates € 13,050,000.³⁷ Moreover, for the year 2009 - in an effort to optimise management - a grouping of the Independent Administrative Authorities (including the CNIL) is expected under a programme called ‘protection of rights and freedoms’.³⁸ Consequently, the CNIL’s credits will no longer be linked to the Department of Justice, but to the group composed of authorities in charge of the protection of freedoms. This should give the CNIL a certain amount of financial autonomy because it will no longer receive any funds from the Department of Justice. It is necessary to underline the fact that the LOLF (Organic Law on financial Legislation) does not authorise the Parliament to adopt amendments to transfer credits from one mission to another within this group, which would add to the financial autonomy of the CNIL.
- [27]. The independent nature of the CNIL is apparent because its decisions may only be challenged through judicial control. The members of the CNIL are elected for terms of five years, renewable once. The members are bound by rules governing conflict of interest. They may not be given instructions from any other authority. No public authority or private entity may interfere with the CNIL’s work; however, they are required to cooperate with the CNIL. Moreover, it is important to highlight that the Commission has complete operational autonomy. Its operations are overseen by the President; its agents are held to the same code of conduct as the members of the Commission, namely with regard to conflict of interest, secrecy and independence.
- [28]. However, Parliament was able to show that the opposition is under-represented – if not absent – in the CNIL. In December 2008, a member of Parliament from the opposition was appointed to the CNIL. Similarly, although certain Independent Administrative Authorities have been given their own legal status, this is not true for the CNIL. In addition, a government commissioner appointed by the Prime Minister, is assigned to the CNIL. He receives all opinions and decisions and may call for a second deliberation to be held within ten days following the initial deliberation (except where sanctions are concerned), but does not take part in voting. This may cause concern about the real independence of the CNIL. It is important to add that the Council of State recently recognised the CNIL as a “court” under the terms of Article 6(1) of the European Convention on Human Rights.³⁹

³⁷ The Ministerial Committee’s annual projections are annexed to the draft finance law for 2009 (*direction de l’action du gouvernement*), p 104.

³⁸ The Ministerial Committee’s annual projections are annexed to the draft finance law for 2009 (*direction de l’action du gouvernement*), p 105.

³⁹ M.-A. Ledieu (2008), ‘La CNIL est une juridiction!’, *Communication Commerce électronique*, n°6, alerte 70 (decision, dated 19.02.2008 of the judge hearing applications for interim relief).

- [29]. With regard to its budget, things are a bit more complicated: the Commission must ‘possess the funds necessary for the successful accomplishment of its missions’ and the Commission itself must draw up a draft budget each year. Similarly, the system for budgetary control differs from that under common law. The importance of the reform expected for the LOLF in 2009 must be recognised. It is clear that financial independence is currently lacking. Some thought does seem necessary. Many European countries have turned to private investment as a solution, and it seems that other possibilities may exist. According to its current President, ‘if the CNIL wishes to achieve total independence with regard to other public authorities, it must radically modify its methods for financing operations – and base its methods for financing on the English model, for example. Everyone in the field of computer science, including the entities that employ these people, could be asked to pay registration fees. The threshold effect must be taken into consideration.’ The idea is not to increase the workforce in Paris but to develop interregional branches, each with a dozen or so employees.
- [30]. The CNIL deliberations are accessible on the *Legifrance* website. Certain private publications (Lamy, Jurisclasseur) equally provide access to these deliberations. Moreover, the most important ones are published on the CNIL website: namely all recommendations, simplified norms, waiver decisions, authorisations, as well as the major deliberations on current events. A certain number of deliberations are also published in the Official Journal. They are available upon request, pursuant to the terms of communication set forth in the CNIL rules of procedure.
- [31]. NGOs’ conduct rights awareness campaigns. They are composed mostly of students, young workers and professionals. Their participation in the performance of studies and creation of networks proves that data protection is a great concern for them. The associations belong to both national and international networks. Their work on the domestic level is closely related to that carried on the global scale.⁴⁰ Major conventions, conferences and forums are organised between them. While these efforts have succeeded in gathering thousands of French nationals, their ability to communicate with laymen has been questioned. In order to improve communications, these associations set up workshops in many universities. On another level, trade unions⁴¹ also protect and monitor possible data protection rights violations. Because they are frequently members of the European Trade Union Confederation,⁴² data protection is an integral part of their agendas. CFDT proposes workshops to

40 IRIS association illustrates this: by being a member of the European Digital Rights federation and closely linked to the *Ligue des Droits de l'Homme*, IRIS targets a vast population, in: <http://www.iris.sgdg.org> and www.ldh-france.org (21.11.2008).

41 The France trade union congress landscape is mainly composed of : *Confédération française démocratique du travail (CFDT)*, *confédération française des travailleurs chrétiens (CFTC)*, *confédération générale du travail (CGT)* and *force ouvrière (FO)*.

42 See ETUC (16.11.2001), « *Première phase de consultation des partenaires sociaux sur la protection des données personnelles des travailleurs* », p.3, in : www.etuc.org (03.12.2008).

employees (and employers) and provides them with information on their rights, namely through the designation of a delegate on data protection, who reports to the CNIL, and the implementation of safety measures, when it comes to data-processing risks⁴³. According to national labour law, a close dialogue must exist between the employers and the Works Council employees' representatives, and the trade unions, whenever the employer wants to implement a new security system that could eventually violate - or at least infringe upon - employees' right to privacy⁴⁴. In practice, however, CNIL reports that a vast majority of employees simply do not know their rights. The paradox is that employers know the existence of this system, but do not apply it: they are reluctant to do so⁴⁵.

- [32]. Many of the law firms that work on data protection cases are in Paris, although a few firms specialised in Criminal computerised law or Law on personal Data and Data processing exist in other parts of the country.

3. Compliance

- [33]. Most of the requests for advice received by the CNIL are related to preliminary formalities. The CNIL does not always respond positively to requests for authorisation; in 2006, while it granted 132 authorisations, it also refused 19, specifically related to checks on employees using fingerprints, certain methods requiring social security numbers, and data-processing using the names. While the CNIL granted 214 authorisations in 2007, it also refused 26.

- [34]. Beginning in 2005, following the modification of the law of 1978, the CNIL multiplied on-site checks as part of an effort to enforce preliminary formalities.⁴⁶ The failure to complete preliminary formalities, before the start of data processing, is common to many cases received by the litigation department; in 2007, 26 per cent of sanctions were related to the failure to complete preliminary formalities. Three decisions to impose sanctions, handed

43 CFDT, *Cadre 'le correspondant informatique et libertés'*, 11.03.2006, <http://www.cadres-plus.net> (15.12.2008).

44 According to another CNIL report by Hubert Bouchet, Vice President of the CNIL, 'collective discussions have to take place before technological change can [?] occur'. *Code du Travail* L-432-2. This includes trade unions since this study was made under the pressure of these very same representatives [translation by the author]. France/CNIL/Report (2004), *'cybersurveillance sur les lieux de travail'*, p. 9 to 10, Summary Report.

45 Recent analysis by CNIL: 'Systems to alert professionals are not often used by companies. Reports frequently show that salaried employees are not informed of their rights. [...] The most obvious example of this is the failure to complete preliminary formalities for the CNIL. The absence of preliminary formalities results from a certain reluctance'. 'Ressources humaines : la CNIL contrôle cinquante entreprises!', <http://www.cnil.fr>, 26/06/2008 (19.11.2008).

46 For example, in 2006, the CNIL conducted an on-site check of the Navigo system, which produces electronic transport cards used by the RATP: it verified the data-processing conditions, and made several observations, in particular during a deliberation on 08.04.2004, and checked the effectiveness of commitments made by different actors involved in the operations.

down at the end of 2006, were appealed before the Council of State. Of the three decisions, the third sanctioned a business for having carried out data processing in a human resources-related operation, including transfrontier data flow, without providing all of the information that the CNIL requested in the form of preliminary formalities. Although these rules were relaxed in 2004, they still seem to be inappropriate today. According to some, the system would gain in efficiency by increasing exemptions from preliminary formalities, which would eliminate some of the heavy administrative work weighing down on the CNIL.⁴⁷

- [35]. The function of the Data Protection Officer (CIL) is described in the 2004 law and the decree dated 20.10.2005⁴⁸, which created the position. He/she may be appointed to the public or private sector. It is possible – where there are fewer than 50 people in the company – to have complete freedom of choice. This person must be independent and may not be pressured by any person responsible for data processing, and may not be sanctioned by his/her employer ‘for reasons related to his/her mission’. If his/her duties are not met, he/she is relieved from the function upon request, or after consultation with the CNIL.
- [36]. The appointment of a CIL has as a consequence a waiver to the preliminary formalities. The Correspondent represents a real deterrent, because he/she has the power to alert the CNIL to any violation of the law. According to statistics included in the 2007 Annual Report, as of 15.12.2007, 1723 organisations had designated a Correspondent. In 2007, more than 1050 organisations notified the CNIL of their decision to appoint a Correspondent (compared to 650, in 2006, and 73, in 2005). The CNIL also organises informational workshops.⁴⁹ A special Correspondents Unit is now a part of the new Management Department for User Relations and Audits at the CNIL, and is at their disposal. More than 80 per cent of CIL come from the private sector and work in industrial enterprises, insurance companies and banks.

4. Sanctions, Compensation and Legal Consequences

- [37]. For all practical purposes, before 2004, sanctions were only imposed by courts. However, ‘there were very few convictions, as the courts were not inclined to

⁴⁷ P. Blanc-Jonason (2008), ‘Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle’, *Actualité Juridique Droit Administratif*, p.2105, which compares the French and Swedish systems.

⁴⁸ France/Decree 2005-1309 (20.10.2005).

⁴⁹ 10 training sessions were conducted in 2006, 17 in 2007 for 650 participants. In 2007, two new theme-based workshops were created: ‘health/social security/medical research’ and ‘local administrations’.

try cases involving this kind of offence'.⁵⁰ Since then, relationships have been established with the Ministry of Justice, and prosecutors, to make the public prosecutor more aware of this type of offence. A recent circular letter from the Department of Justice, dated 04.11.2008, reminds judicial authorities to inform the CNIL of any decision issued applying the law of 1978.

- [38]. The sanctions which may be imposed by the CNIL are described in Articles 45-49 of the revised law. The CNIL may issue warnings and formal notices to those responsible for the processing of personal data who do not comply with the law. 94 such decisions were handed down in 2006. However, it must be pointed out that in 82 per cent of cases, the organisations complied with the demands of the CNIL, which put an end to the sanction proceedings, as set forth by the law.⁵¹
- [39]. Before sanctioning, demands for explanations are made from the person responsible. If explanations are not provided, the CNIL may issue warnings or formal notices, or commence a procedure in which both parties are heard, allowing the person to defend him/herself. The CNIL can also issue pecuniary sanctions or injunctions to order the cessation of processing of personal data or its destruction. Pecuniary sanctions must be proportionate to the seriousness of the violations committed - as well as to eventual profits gained as a result of the violations - and cannot exceed 150,000 €. ⁵² The State cannot be issued injunctions to stop data processing or to destroy data or pecuniary sanctions (in cases of data processing submitted to the obligation of preliminary declaration). Warnings are of public nature, but the public nature of other sanctions is subject to the bad faith of the person in charge of the processing (art. 46).
- [40]. The CNIL may retract authorisations granted pursuant to Article 25 for both public and private sector processing. In certain cases, considered emergencies, such as when there is an offence to rights and freedoms mentioned in Article 1 of the Law on Data Processing, Data Files and Individual Liberties, the CNIL can resort to other measures after the proceedings respecting the defense: stopping data processing or locking up data for a maximum duration of three months. The Commission can also decide to inform the Prime Minister so that he may take action in order to stop violations, without the obligation to make the consequences public. Moreover, in cases where serious violations of rights and freedoms are committed (described under Article 1), the President of the Commission can request a summary judgment from the appropriate court, and,

⁵⁰ C. Pallez (Secretary-General of the CNIL) (2004), 'The exercise of the power to sanction is a real cultural revolution for the CNIL' [translation by the author], *Petites Affiches*, n°195, p.3. He specified that the cases brought before the judge by the CNIL before 2004 ended in a 'simple filing without follow-up or a reminder of the law, whereas the violation should have been sanctioned'.

⁵¹ Extracts from an interview with G. Rosier, Honorary Counselor at the *Cour des comptes*, Commission for Economic Affairs, in: *CNIL Annual Report 2006*.

⁵² Up to 300,000 € for a second offence committed within five years. If the violator is a company, this shall not represent more than 5 per cent of sales.

if necessary, impose any security measures necessary to protect rights and freedoms. The CNIL can refer the case to the Public Prosecutor, which happens only exceptionally. The CNIL does not have the power to enforce restitution payments for damages.

- [41]. Certain authors argue that this arsenal of deterrents is mainly used for dissuasive purposes, which is a polite way to avoid referring to them as theoretical. Proceedings are rare, and violations of existing rules are often settled amicably on the initiative of the CNIL.⁵³ The CNIL underlines the fact that this is a new jurisdictional power, which makes it necessary to establish rules to guarantee the irreproachable nature of the sanctions, and the growth in importance of the system. In 2006, The CNIL imposed 11 pecuniary sanctions for a total sum of 168,000 € (fines ranging from 300 to 45,000 €),⁵⁴ four warnings (issued to a bank, a political party and two telephone companies), seven injunctions to cease or modify the processing of personal data, and 94 formal notices.⁵⁵ In 2007, the CNIL imposed nine pecuniary sanctions for a total of 175,000 € (fines ranging from 5,000 to 50,000 €), five warnings, and 101 formal notices.⁵⁶ It is important to note the real dissuasive effect this has had: the 2007 Annual Report clearly states that the role of the litigation department has become crucial (to the work of the CNIL). Its work is particularly effective, and this benefits all citizens.
- [42]. Criminal sanctions may also be issued along with the sanctions imposed by the CNIL. The President of the CNIL is informed of all criminal proceedings related to offences described under Articles 226-16 - 226-24 of the Criminal Code. The 2004 law goes against a decriminalisation trend apparent in other areas, such as business law.⁵⁷ This criminalisation is coupled with the standardisation of sentences of the highest level: five years of prison and a 300,000 € fine.⁵⁸ When the Commission hands down its final decision for pecuniary sanctions before the criminal judge has issued a final decision on the same facts or related facts, the criminal judge can order that the pecuniary sanction be ascribed to the fine that he decides to impose.
- [43]. In practice, however, these sentences are rarely handed down and are often inferior to what is defined by the law, as the Prosecutors and courts have not

⁵³ D. Forest (2007), 'Pouvoirs de sanction de la CNIL: le réveil soudain de la belle endormie', *Rec. Dalloz*, p. 94.

⁵⁴ The sanctions were aimed at four banks for non-compliance with inspection rules in the databases of the French National Bank [*Banque de France*].

⁵⁵ CNIL, *Annual Report 2006*.

⁵⁶ CNIL, *Annual Report 2007*.

⁵⁷ A. Lepage (2005), 'Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel', *Droit pénal*, n°3, para.16.

⁵⁸ J. Raynaud, 'Informatique et données à caractère personnel', in : *Dictionnaire des droits de l'homme* (dir. J. Andriantsimbazovina et al.), (2008), PUF, Quadrige, p. 527.

been sensitised to these issues.⁵⁹ As the decisions to impose sanctions are reasoned, each case is analysed, so that, pursuant to Article 47 of the law, the seriousness of the violation committed is taken into consideration (one or more, and of what nature?), along with the eventual profit gained from this violation (including economic and technical benefits, or even fame).

- [44]. It is not important how the discovery of the violation is made (complaints received by the CNIL, CNIL initiative, audits executed upon request by the European Union, as the follow-up is always the same - based on the application of administrative or criminal sanctions, pursuant to the law.
- [45]. Unfortunately, there are no statistics on the decisions issued in application of the law of 1978. During complaint investigations, the CNIL frequently intervenes to aid those in litigation with their employer – this is often the case in the employment sector or in companies (communications operator, bank...) - and indirectly works on behalf of the individual. On a very rare basis (less than ten cases per year), a CNIL representative is asked to come before the court as a witness, pursuant to Articles 435-457 of the Code of Criminal Procedure. A profound reorganisation of the CNIL took place on 01.07.2007, with the regrouping of User Relations and Regulatory Services, Complaint Services, Management and Regulation of Sanctions, as well as the service in charge of reception and telephone communications and the Correspondents of data-processing and freedoms in the workplace, under the same management. The goal is to better serve and orient citizens looking for help from the CNIL, in order to guarantee the protection of their rights. Moreover, the CNIL develops partnerships with consumer associations, in order to find ways to intervene at the local level. In conclusion, it is the judge's role in France to decide the distribution of charges in judicial proceedings, and common law rules are applied.
- [46]. Under the 2007 Annual Regulation Program, the Commission wanted checks to be carried out on-site, so that the data-processing systems used for Human Resources purposes could be verified. It must be said that the application of the law on Data Processing, Data Files and Individual Liberties in the field of personnel management, in the broad sense of the term, is representative of a large part of the audits carried out, annually, by the CNIL. Approximately fifty checks were conducted, which allowed for the verification of systems for the processing of personal data, on employees, including computerised management files, and recruitment files, and biometric technology and position determination technology.

⁵⁹ M.-P. Fenoll-Trousseau, 'Protection des données à caractère personnel. Vie privée et communication électronique', *Jurisclasseur Communication*, fasc. 4735, §15.

5. Rights Awareness

- [47]. Knowledge about the CNIL has grown dramatically in the last few years. Awareness campaigns have taken multiple forms. In 2007, the CNIL began by reorganising its website. It held an online poll in November 2007 to solicit the opinions of Internet users. The CNIL also began to work with the media. For example, in October 2007, it joined France Info, creating a weekly programme on data processing and freedoms, part of a show called ‘the right to information’ [*Le droit d’info*]. Moreover, in July 2007, the presentation of the CNIL’s 2006 Annual Report by its President, Alex Türk, was particularly publicised. In 2007, approximately 600 broadcasts cited the CNIL. Programmes such as the ‘*On-site visits across the country*’⁶⁰ were also organised. In 2007, the Annual Report underlined that ‘agents and members of the CNIL participated in 155 symposia, seminars, conferences or interactive training programs on the law on Data Processing, Data Files and Individual Liberties, or on the function of the Data Protection Officers within companies, administrations, and local authorities’. The CNIL also increased its communication with companies, through the network of Chambers of Commerce and Industry (AFCCI), with which it has signed an agreement, and organised regional meetings, for training purposes.
- [48]. According to a survey conducted by SOFRES (French Society on poll studies) in January 2008,⁶¹ 61 per cent of French people think that collecting data is a violation of their right to privacy, and they consequently desire more protection. Moreover, if only 34 per cent of the population knew that this agency existed in 2004, there are 16 per cent more in 2008. According to studies conducted by TNS SOFRES, upon request by the CNIL, in a study of 1,000 people, 32 per cent claimed to know about the CNIL in June 2004, 37 per cent in December 2005, 39 per cent in December 2006, and 50 per cent in November 2007.⁶² One person out of two knows about the CNIL, and the tasks that it performs. However, few of them know their rights in terms of data protection, though a significant communications network has been established between the CNIL, jurists, associations and trade unions. According to a poll taken by TNS SOFRES, which was requested by the CNIL, 26 per cent of the 1,000

⁶⁰ Initiated in January 2005, this new system for information and communication allowed for contact with approximately 7,000 people : companies, administrations, local authorities, elected officials, associations, journalists, citizens, lawyers, healthcare and education professionals, social workers, etc.; 14 regions were visited between 2005 and 2007.

⁶¹ Sofres, 25/01/2008, « 61% of French people believe that the creation of computerized data files infringes upon their right to privacy », in: <http://www.cnil.fr> (19.11.2008).

⁶² CNIL, *Annual Report 2007*, p.39.

questioned said that they had been sufficiently informed about their rights with regard to the protection of personal data.⁶³

- [49]. The growth of the CNIL's reputation in 2007 (+11 per cent) can be explained by its continued exposure. In order to better help citizens understand their rights, the CNIL, through publications on its website and broadcasting, is opting for more practical means of communication (examples of real situations, questions/answers, campaigns to spread awareness about tracking). Certain initiatives deserve to be mentioned: some agreements and partnerships signed by the CNIL with the Association of the Universities' Chairpersons (CPU), on 25.01.2007, the partnerships with the HALDE (the French Equal Opportunities and Anti-Discrimination Commission), established on 03.05.2006. Also, there was the creation of the network of CIL in higher education in December 2007, as well as the convention that may be signed with the CNC (National Commercial Council), to aid in the protection consumers' personal data.

⁶³ CNIL, *Annual Report 2007*, p.39.

6. Analysis of deficiencies

- [50]. Firstly, the CNIL has written to the Expert body chaired by Simone Veil in charge of drafting changes of the Constitution, to recommend the insertion of the right to the protection of personal data (in the strict sense of the word), the right to privacy, and the right to identity, into the corpus of the Constitution. On another level, the CNIL is concerned about the increase of legislation related to personal information (the CNIL dedicates 90 per cent of its time to this problem, known as the legislative ‘tidal wave’).
- [51]. Secondly, with regard to operational problems, the CNIL gives citizens the right to access a certain number of police databases, namely the Data processing on registered offences (STIC). This computerised file must be adapted so that the data may be modified in real time, especially after discharges are granted. A person wrongly listed on the STIC could lose his/her job or be refused a position in the security sector due to the existence of old information in this database. With regard to the Intelligence Services (RG), there is less of an issue. After the Bruno Rebelle case⁶⁴, the CNIL was overrun with requests for access to this database, which mainly came from two categories of people: journalists and members of Parliament. These people were often upset to find out that a file, containing a few pieces of information, existed in their name. More generally, the privileged status of State databases is debatable – the CNIL has almost no a posteriori regulatory control over State databases under Articles 26 and 27.
- [52]. With regard to the theoretical nature of sanctions, it seems that the CNIL’s lack of resources, combined with the small number of complaints brought, explains the low number of sanctions issued. ‘Thirty years after the vote on the law, one cannot say that the French understand the law of 1978.’⁶⁵ There is an ‘insufficient level of individual and collective knowledge of the real and new risks for individual freedoms’.⁶⁶
- [53]. On the whole, the CNIL is an institution which seems to be under-supported in the political world, and isolated in its national struggles.⁶⁷ The Commission in charge of studying the possibilities for institutional reform, whose work led to an amendment to the Constitution in the summer of 2008, recommended the breakdown of the CNIL and the creation of a ‘Fundamental Rights Defender’,

⁶⁴http://tempsreel.nouvelobs.com/speciales/elections_2007/20070125.OBS8835/la_note_des_rg_sur_bruno_rebelle.html (28.01.2009).

⁶⁵ J. Frayssinet (2008), ‘Dossier spécial Loi « Informatique et Libertés », Les trente ans de la loi « Informatique et libertés’, *Revue Lamy Droit de l’Immatériel*.

⁶⁶ J. Frayssinet (2008), ‘Dossier spécial Loi « Informatique et Libertés », Les trente ans de la loi « Informatique et libertés’, *Revue Lamy Droit de l’Immatériel*.

⁶⁷ J. Frayssinet (2008), ‘Dossier spécial Loi « Informatique et Libertés », Les trente ans de la loi « Informatique et libertés’, *Revue Lamy Droit de l’Immatériel*.

which would regroup several authorities, and reduce its role to that of a mediator. These debates led the CNIL to create a working group assigned to make proposals for reform; its conclusions are due in the near future.

- [54]. With regard to data, Article 2(2) of the law has led to diverse interpretations. French judges have taken contradictory positions in litigation involving the collection and processing of IP numbers, through data exchanges using peer-to-peer file-sharing software. The Court of Appeals of Paris stuck to a narrow interpretation, which is not adapted to new technologies.⁶⁸ The notion of ‘processing’ is also unclear. In this regard, the legislature should intervene. A decision from the Court of Cassation which would resolve these questions is expected. The CNIL has also requested to appeal to the highest instance, in the interest of the law, following decisions issued by the aforementioned Appeals Court.
- [55]. The rules for the publication of CNIL Opinions should be revised so as to guarantee that Parliament is fully informed when it must respond to questions on the protection of data. The CNIL attracted the attention of public authorities to the incoherent nature of a system that allows for Opinions to be issued that may never be known, if the government does not want them to.⁶⁹
- [56]. According to the current President of the CNIL, ‘the formalities of declaration are still poorly understood, as they are too complex, trans-frontier data flow is not really covered in the law, the information given to people on their rights should be more explicit, and internal procedures should be reconsidered, so as to make (the Commission’s) work more efficient and rapid (...)’.⁷⁰ Following a study conducted by the CNIL on methods to calculate diversity, it became obvious to the Commission that the law on Data Processing, Data Files and Individual Liberties needed to be modified, in order to better guarantee the protection of individuals and of their sensitive data, by making sure that research conducted on discrimination is of a scientific nature. It also decided that the CNIL’s regulatory control over computerised data files used for research purposes needed to be reinforced, and that more than the individual’s consent should be required with regard to these files. Moreover, it seems necessary to clarify the rules related to video surveillance and especially to standardise, or even unify, the rules on formalities (between the CNIL and the departmental commissions on video surveillance).⁷¹ The attribution of the

⁶⁸ France/Cour d’Appel Paris/ 13° ch. Corr./sect. B (27.04.2007).

⁶⁹ In the HADOPI bill (protection of copyright and peer-to-peer software), for example, the CNIL was not able to issue an opinion on the text, which was the subject of a Parliamentary debate, as it was not able to support its argument using information that the Government did not wish to have publicised.

⁷⁰ A. Türk (2008), ‘La loi “Informatique et Libertés”, 30 ans après: quel bilan?’, *Revue Lamy Droit de l’Immatériel*.

⁷¹ The law dated 21.01.1995, was passed at a time when video surveillance was essentially carried out by analogous recording onto magnetic tape. Today, it must be revised, given the evolution of technology, such as the filing and storing of videos on web servers. In addition, the two different

power to regulate video surveillance systems to the CNIL - whatever the place of installation may be - is an interesting idea, proposed by the CNIL itself.

- [57]. However, it is true that the majority of deficiencies are linked to insufficient resources, in spite of progress made in this area over the last few years. It must be said that this progress has not allowed the CNIL to reach the European average.

7. Good practices

- [58]. Among the various successful informational and advisory campaigns conducted by the CNIL, the war against 'spam' or unsolicited e-mail, in place since May 2007, should be mentioned. Its objective is to collect and process the complaints of Internet users, and to direct them to the different actors involved in the war against 'spam', such as public and political authorities and professionals, according to their diverse missions and capabilities.⁷² Signal Spam (the French National Spam Hotline) can bring a complaint before the CNIL against a 'spammer', so that it may use its powers to regulate and sanction.
- [59]. As part of its informational and advisory missions, the CNIL participated in an event organized by the European Council on 28.01.2007: the first European Data Protection Day, in order to create awareness among citizens to the number of actions in everyday life (using the telephone, using one's bank card or surfing the Internet) which generate traces containing information about our identity.
- [60]. The CNIL's involvement on the international scene should also be mentioned, especially because, since February 2008, its President is also the president of the Article 29 Working Party.
- [61]. In October 2008, in collaboration with its German counterpart, CNIL organized the 30th global conference of authorities on the protection of data and privacy; it was held in Strasbourg from October 15-17. In this fashion, it was able ensure the adoption of several resolutions, on the urgent need to adopt international standards on the protection of data, the on-line privacy of children, and the protection of privacy with regard to social networking services.
- [62]. Lastly, in 2008, for the first time, a doctoral prize '*Data Processing, Data Files and Individual Liberties*' was created by the CNIL, in the amount of 7,000 Euros, and the proposal submitted by the CNIL - in collaboration with its German counterpart - for the creation of a Noble Prize in the field of Data

sets of rules governing video surveillance in the public and private sectors are neither clear, nor easily understandable.

⁷² See partnership agreement signed on 30.10.2007 between the CNIL and the association Signal Spam.

Protection and Liberties, was approved during the conference at Strasbourg, and will be a reality by 2010.⁷³

- [63]. As part of its watchdog and forecasting activities, the contributions of the CNIL on standardisation projects, particularly with regard to security, and its involvement as a member of the consortium and steering committee on national and international research projects (See *Annual Report 2007*, p 50), also deserves to be mentioned.

⁷³ IPA Declaration « International Privacy Association » on the creation of a Nobel Prize in the field of Data protection and liberties, to be awarded annually by the global conference of authorities on the protection of data. http://www.privacyconference2008.org/index.php?langue=2&page_id=1 (12.12.2008).

Annexes

Annex 1 – Tables and Statistics

Please complete the table below

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority				6,478	6,9	7,12	9,0	9,9
Staff of data protection authority				76	80	85	95	105
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	controls: 30	controls:30	controls:52	controls:31	controls:45	controls:96	controls:127	controls:164

	2000	2001	2002	2003	2004	2005	2006	2007
Number of data protection registrations	52843	50089	54128	65921	66840	80677	73800	56404
Number of data protection approval procedures							132 19 of which were refused	214 26 of which were refused
Number of complaints received by data protection authority ⁷⁴	3399	3574	5076	3567	3591	3834	3572	4455

⁷⁴ The evolution in the number of complaints deserves to be commented upon : on the one hand, the establishment of new tools in the form of *guides sectoriels* for users, and awareness campaigns have had a limiting effect (on the number of violations) and have, at the same time, led to an increase in the number of complaints; on the other hand, the creation of the front office telephone and postal service (SORP) within the CNIL, has helped to redirect complaints or to resolve problems before they are classified as complaints. The CNIL can be sure that (given the rise in activity) the number of complaints would have exploded without the help of the front office.

Number of complaints upheld by data protection authority ⁷⁵								
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)						warning issued:2 sanction issued: 0	warning issued:4 sanction issued: 11	warning issued:5 sanction issued: 9
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible,								

⁷⁵ There is no indication in the CNIL system of the number of complaints processed. Nevertheless, an internal CNIL study showed a rate of 80% of processed complaints, which includes closed cases, and those in process, in relation to the number of complaints received.

please disaggregate between sectors of society and economy) ⁷⁶								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	Warning(0), Denuncia- tion to the Public Prosecutor (1)	Warning(0), Denuncia- tion to the Public Prosecutor: (1)	Warning(2), Denuncia- tion to the Public Prosecutor: (7)	Warning(5), Denuncia- tion to the Public Prosecutor: (9)	Warning(7), Denuncia- tion to the Public Prosecutor: (2)	Warning(2), formal notice(27), financial sanction(0), <i>injunction</i> <i>na</i> *; Denuncia- tion to the Public Prosecutor: <i>n</i> <i>a</i> *	Warning(4), formal notice(73), financial sanction(11), injunction(7), Denunciation to the Public Prosecutor: <i>na</i>	Warning(5), formal notice(101), financial sanction(9), injunction(2) ; Denunciation to the Public Prosecutor:(5)

⁷⁶ The CNIL does not follow-up on the application of decisions to sanction or the fines imposed by the court. It does, however, communicate warnings to the prosecutor as well as information on appeals of decisions issued by the CNIL. The warnings are communicated to the prosecutor by mail, and signed by the President of the CNIL before the appropriate court, and follow-up is guaranteed, pursuant to Article 52 of the law, dated January 6, 1978 modified on August 6, 2004 : ‘The public prosecutor shall inform the chairman of the CNIL of any legal proceedings in connection with breaches of the provisions of Section 5 of Chapter VI of Title II of Book II of the Criminal Code and, when appropriate, the decisions taken in respect of them. He shall inform him of the date and purpose of the court hearings by a registered letter with advice of delivery sent at least ten days before that date’.

*na : unavailable

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Case title	M. Skandrani case
Decision date	7 April 2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Arrêt n° 275216 du Conseil d'Etat</i> (Judgement n. 275216 of the French Council of State). The Council of State advises the government on the preparation of governmental bills, statutory laws, and certain decrees. The Council of State is also the highest administrative jurisdiction – it is the judge of last instance for cases regarding executive power, local authorities, independent public authorities, public administration agencies, or any other agency wielding public authority.
Key facts of the case (max. 500 chars)	In 2004, Mr. S., a French national, made an application to the French Data Protection Authority (CNIL) in order to have data concerning himself in the Schengen Information System (SIS) deleted. He claimed that this data had been unlawfully stored by German authorities. The CNIL addressed the competent German supervisory authority, which replied that the inclusion of the alert in the Schengen Information System was lawful from the point of view of the Data Protection Law. On this basis, the CNIL considered that the proceedings concerning the applicant had ended. On 13 December 2004, the applicant attacked this decision before the <i>Conseil d'Etat</i> for misuse of power.

<p>Main reasoning/argumentation (max. 500 chars)</p>	<p>The Council of State [<i>Conseil d'Etat</i>] recalled that (according to Articles 6 and 114 of the Convention on the application of Schengen Agreement) the CNIL must carry out an investigation on such an alert in close coordination with the supervisory authority of a given State, when it receives an alert about unlawful registration in SIS. The CNIL cannot transfer its responsibilities to the latter. Moreover, the CNIL must request all information required to perform its regulatory tasks. In case of objection, the CNIL must refer the matter to the joint supervisory body.</p>
<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>The Council of State held that in the current case the CNIL has insufficient information to properly carry out its regulatory duties. In addition, the Council of State ordered the CNIL to resume the regulatory process related to the plaintiff.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The <i>Conseil d'Etat</i> set aside the decision <i>de quo</i> and ruled that the CNIL was to resume its regulatory mission in close coordination with the competent German supervisory authority. When the CNIL receives a request to delete data in SIS from another Convention member State (other than France) it must carry out a thorough check and decide whether or not to approve the registration.</p>
<p>Proposal of key words for data base</p>	<p>Schengen Information System (SIS); Germany; Trans-frontier Data processing</p>

Case title	Constitutional scrutiny of: <i>Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés</i> (Act of 6 August 2004 related to the protection of individuals with regard to the processing of personal data, amending Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties)
Decision date	29 July 2004
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Décision n° 2004-499 DC du Conseil constitutionnel</i> (Decision n. 2004-499 DC of the French Constitutional Court)
Key facts of the case (max. 500 chars)	On 20 th July 2004, more than 60 deputies contested Articles 8, 9, 21, 22 and 26 of the above-mentioned Act, in particular Article 9, which provides information on companies for the collection and distribution of authors' royalties (Paragraph 4) and all professional victims of fraud (Paragraph 3) to put in place processing of personal data related to offences, convictions and security measures in order to curb copyrights piracy.
Main reasoning/argumentation (max. 500 chars)	Paragraphs 3 and 4 would allow a private legal person and the companies for the collection and distribution of authors' royalties to collect a huge amount of personal data concerning offences, convictions and security measures. Given the magnitude of such processing and the nature of the information, the deputies hold that citizens' fundamental freedoms/rights/liberties and respect for private life (privacy) would be put in danger. Moreover, they argue that the object and conditions of Paragraph 3's mandate are vague and imprecise, especially with regard to the term 'fraud'.

<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>Paragraph 3 neither gives a definition of ‘fraud’ nor lists which offences it consists of. It does not explain what may be done with the information, whether it can be transferred and how long it shall be stored. Paragraph 4 aims to fight against new counterfeiting techniques and to safeguard intellectual property. The information gathered cannot be used in a legal proceeding. The balancing of interests in this second case is not disproportionate.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The <i>Conseil Constitutionnel</i> affirms that the text of this Act is fundamentally constitutional. However, it repeals Paragraph 3 of Article 9 and states that Paragraph 4 is constitutional under the condition that the prohibition on the creation of private databases of offences shall not prejudice people’s right to sue.</p>
<p>Proposal of key words for data base</p>	<p>respect for private life - processing of personal data by certain legal persons – copyright royalties - fight against fraud, piracy and counterfeiting</p>

Case title	<i>Crédit Lyonnais</i> (LCL) case
Decision date	28 June 2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Délibération</i> n° 2006-174 du CNIL, <i>Commission nationale de l'informatique et des libertés</i> (Resolution n. 2006-174 of the CNIL) Founded by the law of January 6, 1978, the CNIL is an independent administrative authority dedicated to the protection of the right to privacy and personal data.
Key facts of the case (max. 500 chars)	On different dates in 2004 and 2005, four applicants filed a complaint with the CNIL against <i>Crédit Lyonnais</i> on the legality of their registration by the latter in two central files of the French National Bank. As the CNIL's requests for further information and data were not properly complied with by Credit Lyonnais, the CNIL was forced to conduct audit inspections of <i>Credit Lyonnais'</i> information systems. These investigations showed some inconsistencies between the data communicated by <i>Credit Lyonnais</i> and that recorded in its computerised data filing systems.
Main reasoning/argumentation (max. 500 chars)	The CNIL based its Resolution on Article 21 Paragraph 2 and Article 51 of Act 78-17. Article 21, Par. 2, which sets forth the obligation for institutions which keep personal data files to fully cooperate with the CNIL, so that it may perform its duties. Article 51 establishes penalties for, <i>inter alia</i> , communicating information that does not correspond to the content of the records existing at the time of the request.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	This Resolution clearly recognised that <i>Crédit Lyonnais</i> , like any Institution that keeps personal data files is obligated to collaborate with the CNIL and that such an obligation also requires it to undertake positive actions. Moreover, the CNIL held that the conduct of <i>Crédit Lyonnais</i> in the instant case amounts to acting in bad faith. In the CNIL's view, this factor calls for additional sanctions.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Credit Lyonnais was fined 45,000 € for its repeated failures to observe the obligation of collaboration with the CNIL. As additional sanction for the bank's conduct in bad faith, the CNIL ordered the instant Resolution to be published in two major national newspapers.

Proposal of key words for data base	Collaboration Duty – Bad Faith – Data communication – Positive obligations upon Institutions which keep personal data files
--	---

Case title	Young lawyers' Conference and al. (<i>Fédération nationale des unions de jeunes avocats –FNUJA– et autres</i>)
Decision date	24 January 2001
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Arrêt n° 212484 du Conseil d'Etat</i> (Judgement n. 212484 of the French Council of State) The Council of State advises the government on the preparation of governmental bills, statutory legislation and certain decrees. The Council of State is also the highest administrative Court – it is the judge of last instance for cases regarding executive power, local authorities, independent public authorities, public administration agencies, or any other agency wielding public authority.
Key facts of the case (max. 500 chars)	The FNUJA and others brought their case before the Council of State to request the annulment of the Order of 18 June 1999, establishing the use of automated data-processing systems for the monitoring of criminal proceedings by the Prosecutor's Office of the Courts of Appeal. This order was issued in execution of the Decree 90–115 and established that judicial institutions could introduce systems for the automated retention of personal data related to, <i>inter alia</i> , ethnic origin, political, philosophical or religious opinion, and trade-union membership of the 'parties to the action'.
Main reasoning/argumentation (max. 500 chars)	The Council of State held that the persons subjected to imprisonment on remand, the defendants, the accused as well as the assisted witnesses must be regarded as 'parties to the action' according to the above-mentioned decree. On the other hand, it considered that the persons involved during a preliminary investigation before indictment or an (inquiry of flagrancy) do not necessarily have such a status.

<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>Because of that, the <i>Conseil d'Etat</i> ruled that the order of 18 June 1999 misinterpreted the above-mentioned decree insofar as it allows for the recording and computerised storage of personal data related to the violations of accused persons in preliminary investigations before the indictment or (inquiry of flagrancy)</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The Order of 18 June 1999 is not taken into account to the extent indicated above. The judgement highlights the scope of the Data Protection Regime in France within the framework of criminal proceedings.</p>
<p>Proposal of key words for data base</p>	<p>Judicial Proceedings – Parties in Action – Data Protection – French Privacy Data Act</p>

Case title	TYCO HEALTHCARE FRANCE case
Decision date	14 December 2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Délibération n° 2006-281 du CNIL - Commission nationale de l'informatique et des libertés</i> (Resolution n° 2006-281 of the CNIL) Founded by the law of January 6, 1978, the CNIL is an independent administrative authority dedicated to the protection of the right to privacy and personal data.
Key facts of the case (max. 500 chars)	Tyco notified the CNIL in 2004 that it was operating a human resources database containing personal information, as required by the law. When, at a later date, the CNIL requested further information from the company, Tyco said that it had stopped using the database. An inspection in 2006 by the CNIL found not only that the database was still active, but that it was being used more extensively than the company had indicated. The CNIL raised questions with Tyco about the destination of data, the reasons for international transfers and the safety and security of the data on the network.
Main reasoning/argumentation (max. 500 chars)	The CNIL held that, because of its regulatory role, it must be informed of the real purposes of the processing, the time when personal data is sent to the UK or the US, where the servers and systems are installed, the specific use of the application, the addressees of the information, the security measures ensuring confidentiality and the data retention period. A reply merely mentioning the “reporting” aim of the transfer is considered non-satisfactory.

<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>A fundamental principle of European data protection is that personal information is only shared with countries with equally stringent protections. Data protection authorities shall be informed of personal data transfer across borders and the pertinence of data safeguards.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>Tyco was fined 30,000 EUR and the CNIL enjoined Tyco to reply to the questions raised within ten days. The instant Resolution is ordered to be published. It is believed to be the first time that a US-based multinational has been fined for unauthorised overseas transfers of personal data.</p>

Case title	SERVICE INNOVATION GROUP FRANCE (SIG) case
Decision date	11 December 2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Délibération n° 2007-374 du CNIL - Commission nationale de l'informatique et des libertés</i> (Resolution n° 2007-374 of the CNIL) Founded by the law of January 6, 1978, the CNIL is an independent administrative authority dedicated to the protection of the right to privacy and personal data.
Key facts of the case (max. 500 chars)	On 6 th December 2006, the CNIL carried out an audit of the SIG's staff management procedures. It was discovered that applicants for vacancies could fill out a <i>curriculum vitae</i> online using a data collecting form. This form did not contain the information provided for by Art. 32. Furthermore, some applicants and current or previous employees were listed as 'PNG' (non guaranteed people); no reasoning was given, but many irrelevant and subjective commentaries were attached, such as 'liar', 'hopeless', 'boring', 'stinky', 'pregnant', 'M.'s friend - untrustworthy', 'G.'s wife'. No data retention period was fixed.
Main reasoning/argumentation (max. 500 chars)	Several Articles of Act n°78-17 are invoked. In particular, Art. 6, Par. 1, 3 and 5, provide that processing may be performed only on personal data obtained and processed fairly and lawfully; such data shall be adequate, relevant and not excessive in relation to the purposes for which it is obtained; and shall be stored for a period no longer than is necessary. The data subject must be informed of the purposes of the processing for which the data is intended (Art. 32, Par. 1-3) and is entitled to interrogate the data controller of personal data in order to obtain communication of the personal data relating to him as well as the origin of the data (Art. 39, Par. 4).

<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>Processing of personal data shall not affect irrelevant personal behaviours, employees' health status, personal or family relations, tendency to steal, etc. The sole purpose allowed for the processing is to test applicant or employee's competence to carry out tasks (Art. L.121-6 of the French Employment Code). A data retention period shall always be fixed and justified in regard to the purpose of the processing.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The CNIL required the SIG to comply with the law on data protection and to provide guarantees for the future. Since the second audit carried out by the CNIL certified the SIG failed to do so, the latter was fined 40,000 EUR. The CNIL decided the SIG was not acting in bad faith but ordered the instant Resolution to be published.</p>
<p>Proposal of key words for data base</p>	<p>Staff treatment - inadequate, irrelevant and excessive personal data – right to information – data retention period</p>

Case title	FAC INTERNATIONAL case
Decision date	31 January 2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Délibération n° 2008-029 de la CNIL - Commission nationale de l'informatique et des libertés</i> (Resolution n° 2008-029 of the CNIL)
Key facts of the case (max. 500 chars)	In 2006, an applicant filed a complaint with the CNIL against FAC INTERNATIONAL about the conditions under which the latter had selected her for door-to-door insurance sales directed at foreign people. Following an on-site check, the CNIL found out that the company had bought IMPACT NET from another company (which was also condemned by the CNIL in the same case) , which is a data file containing a list of addresses of people of supposed African and Northern African origin living in France. This dossier was created by compiling a list of foreign-sounding names.
Main reasoning/argumentation (max. 500 chars)	The CNIL based its Resolution on Articles 3 and 8 of Act 78-17. Article 3 sets forth that the data controller is a person, public authority, department or any other organisation who determines the purposes and means of the data processing. Article 8 provides that the collection and processing of personal data that reveals (directly or indirectly) the racial and/or ethnic origins, or political, philosophical, or religious opinions or trade union affiliation of individuals, or which concerns their health or sexual life, is prohibited.

<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>The CNIL stated that having ordered and bought the address list file for direct marketing purposes, the FAC INTERNATIONAL was responsible for the personal data contained in it. Moreover, the company violated Art. 8 since it was aware of the fact that the file revealed the racial and ethnic origins of the data subjects and the latter was the main reason for buying and using such a file.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The CNIL ordered the FAC INTERNATIONAL to pay a fine of 30,000 EUR, which was reduced to 15,000 EUR, given its turnover. The CNIL decided the FAC INTERNATIONAL was not acting in bad faith but ordered the instant Resolution to be published.</p>
<p>Proposal of key words for data base</p>	<p>racial and ethnic origins – responsibility for data protection processing</p>

Case title	Constitutional scrutiny of: <i>Loi pour la sécurité intérieure</i> (Internal Security law)
Decision date	13 March 2003
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	<i>Décision</i> n° 2003-467 DC <i>du Conseil constitutionnel</i> (Decision n. 2003-467 DC of the French Constitutional Council)
Key facts of the case (max. 500 chars)	On 14 th February 2003, more than 60 deputies contested, <i>inter alia</i> , Articles 21 and 25 of the above-mentioned law. Article 21 allows the police to use systems for the automated processing of personal data with regard to the information gathered during the enquiries, in order to facilitate the evidence gathering, the tracking of violations and perpetrators. Article 25 allows for the consultation of the files containing such information for administrative purposes.
Main reasoning/argumentation (max. 500 chars)	The deputies hold Articles 21 and 25 would undermine the protection of privacy. Moreover, allowing consultation of personal data for administrative enquiry, the legislature would permit these data to be used in infringement to the rights of the concerned persons; especially concerning foreigners' application for a residence permit (or its renewal). Lastly, the fundamental principles on the protection of minors in criminal law would be violated as well as the presumption of innocence and principle of equality.

<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>The law on data protection must apply to police files. An administrative decision ‘on a human’s behaviour’ must not be exclusively founded on the automated processing of personal information collected by the police ‘which defines the profile or personality of the person concerned’. Consultation of police files during the renewal of residence permits must not call into question the right to privacy. The retention period for minors will take into account the necessity to find the offenders and the re-education of minors.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The Constitutional Council declared Articles 21 and 25 constitutional under the conditions listed in the previous paragraph (Key issues). Furthermore, it affirms that the presumption of innocence has not been disregarded inasmuch as any person has the right of access and rectification of its own personal data. Finally, it states the principle of equality has been respected and no argument has been proposed by the deputies to justify their complaint.</p>
<p>Proposal of key words for data base</p>	<p>respect for private life - processing of personal data collected during police activities for administrative purposes - juvenile criminal responsibility on the grounds of age - presumption of innocence</p>

Section du
contentieux sur la
rapport de la 10ème
sous-section
Séance du 24 mars
2006 Lecture du 7
avril 2006
N° 275216
M. S.

Texte intégral

[► Lire l'analyse](#)

Vu la requête, enregistrée le 13 décembre 2004 au secrétariat du contentieux du Conseil d'Etat, présentée par M. Manar Mohamed S. ; M. S. demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir la décision du 12 octobre 2004 de la commission nationale de l'informatique et des libertés prise sur sa demande tendant d'une part à ce que lui soient communiquées les informations le concernant figurant dans le système informatique national du Système d'Information Schengen et d'autre part à ce que ces données soient rectifiées ou effacées ;

2°) de mettre à la charge de l'Etat le versement d'une somme de 2 500 euros au titre des dispositions de l'article L. 761-1 du code de justice administrative ;

Vu les autres pièces du dossier ;

Vu la loi n° 73-1227 du 31 décembre 1973 autorisant la ratification de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ensemble le décret n° 74-360 du 3 mai 1974 qui en porte

publication ;

Vu la loi n° 91-737 du 30 juillet 1991 autorisant l'approbation de la convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des Etats de l'Union économique du Benelux, de la République fédérale d'Allemagne, de la République française, relatif à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990, ensemble le décret n° 95-304 du 21 mars 1995 qui en porte publication ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée notamment par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 95-577 du 6 mai 1995 relatif au système informatique national du Système d'Information Schengen dénommé N-SIS ;

Vu le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Edouard Geffray, Auditeur,
- les conclusions de Mlle Célia Verot, Commissaire du gouvernement ;

Considérant que M. S. demande l'annulation pour excès de pouvoir de la décision du 12 octobre 2004 par laquelle la commission nationale de l'informatique et des libertés lui a fait savoir, en réponse à sa demande tendant, d'une part, à ce que lui soient communiquées les informations le concernant contenues dans le système informatique national du Système d'Information Schengen et, d'autre part, à ce qu'elles soient effacées, que l'un des membres

de la commission avait procédé aux vérifications demandées en application de l'article 41 de la loi du 6 janvier 1978 modifiée et que la procédure était désormais terminée ;

Considérant que l'article 92 de la convention signée le 19 juin 1990 à Schengen institue un "Système d'Information Schengen" composé d'une partie nationale auprès de chacune des Parties contractantes et d'une fonction de support technique ; que ce système a pour objet, conformément à l'article 93 de cette convention, de préserver l'ordre et la sécurité publics y compris la sûreté de l'Etat, et l'application des dispositions de la convention sur la circulation des personnes sur les territoires des Parties contractantes à l'aide des informations transmises par lui ;

Considérant qu'aux termes de l'article 110 de la convention : " Toute personne peut faire rectifier des données entachées d'erreur de fait la concernant ou faire effacer des données entachées d'erreur de droit la concernant. " ; qu'en vertu du paragraphe 1 de l'article 114 : " Chaque Partie contractante désigne une autorité de contrôle chargée, dans le respect du droit national, d'exercer un contrôle indépendant du fichier de la partie nationale du Système d'Information Schengen et de vérifier que le traitement et l'utilisation des données intégrées dans le Système d'Information Schengen ne sont pas attentatoires aux droits de la personne concernée (...) " ; qu'il est spécifié au paragraphe 2 du même article que : " Toute personne a le droit de demander aux autorités de contrôle de vérifier les données la concernant intégrées dans le Système d'Information Schengen ainsi que l'utilisation qui est faite de ces données. Ce droit est régi par le droit national de la Partie contractante auprès de laquelle la demande est introduite. Si les données ont été intégrées par une autre Partie contractante, le contrôle se réalise en étroite coordination avec l'autorité de contrôle de cette Partie contractante. " ; que selon l'article 106 : " 1. Seule la Partie contractante signalante est autorisée à modifier, à compléter, à rectifier ou à effacer les données qu'elle a introduites./ 2. Si une des Parties contractantes qui n'a pas fait le signalement dispose d'indices faisant présumer qu'une donnée est entachée d'erreur de droit ou de fait, elle en avise dans les meilleurs délais la

Partie contractante signalante qui doit obligatoirement vérifier la communication, et si nécessaire, corriger ou effacer la donnée sans délai./ 3. Si les Parties contractantes ne peuvent parvenir à un accord, la Partie contractante qui n'est pas à l'origine du signalement soumet le cas pour avis à l'autorité de contrôle commune visée à l'article 115, paragraphe 1 " ;

Sur les conclusions aux fins d'indemnités :

Considérant que M. S. s'est désisté de ses conclusions tendant à la condamnation de l'Etat à lui verser une somme de 50 000 euros en réparation du préjudice subi ; que rien ne s'oppose à ce qu'il en soit donné acte ;

Sur le refus de communiquer les informations concernant M. S. :

Considérant que M. S. a eu, dans le cadre de l'instruction écrite devant le Conseil d'Etat, communication des informations concernant son inscription dans le système informatique national du Système d'Information Schengen ; que, dès lors, les conclusions de sa requête tendant à l'annulation pour excès de pouvoir de la décision de la commission nationale de l'informatique et des libertés en tant qu'elle lui refuse la communication de ces informations sont devenues sans objet ;

Sur l'effacement des données concernant M. S. :

En ce qui concerne les conclusions dirigées contre le refus de rectifier le signalement opéré par les autorités françaises :

Considérant que par son mémoire du 24 octobre 2005, le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire a fait savoir qu'il avait procédé à la suppression du signalement de M. S. dans le système informatique français du Système d'Information Schengen, opéré par ses services en

application de l'article 96 de la convention du 19 juin 1990 relatif aux données relatives aux étrangers signalés par un Etat aux fins de non-admission sur son territoire ; que dès lors, les conclusions présentées sur ce point par M. S. sont devenues sans objet ; qu'il n'y a, par conséquent, plus lieu d'y statuer ;

En ce qui concerne les conclusions dirigées contre le refus de rectifier le signalement opéré par les autorités allemandes :

Sans qu'il soit besoin d'examiner les autres moyens de la requête ;

Considérant qu'en application des stipulations précitées de l'article 106 de la convention du 19 juin 1990, il incombe aux autorités françaises, saisies par une personne qui conteste son inscription dans le système informatique national du Système d'Information Schengen, de procéder, dans le cas d'un signalement opéré par la France, à l'effacement des données entachées d'erreur de droit ou d'erreur de fait ; que, dans le cas d'un signalement opéré par un Etat Partie autre que la France, il appartient à l'autorité de contrôle française, dès lors qu'elle estime disposer d'indices faisant présumer qu'une donnée est entachée d'erreur de droit ou de fait, d'en aviser les autorités de cet Etat ;

Considérant qu'il ressort également des stipulations des articles 106 et 114 de la convention que la commission nationale de l'informatique et des libertés, lorsqu'elle saisit l'autorité de contrôle d'un Etat signalant en vue de la vérification et de l'effacement d'une inscription, est tenue de procéder à l'examen de ce signalement en étroite coordination avec celle-ci, sans que sa responsabilité puisse être transférée à l'autorité requise ; qu'elle doit demander l'ensemble des informations lui permettant de procéder à ce contrôle, et, en cas de désaccord avec l'autorité requise, saisir l'autorité de contrôle commune mentionnée par le paragraphe 3 de l'article 106 ; que si, dans certains cas limitativement énumérés par la convention, la commission nationale de l'informatique et des libertés est tenue de ne pas communiquer au demandeur les informations le concernant, ces stipulations ne font pas obstacle à ce qu'elle exerce son contrôle sur le bien-

fondé du signalement en " étroite coordination " avec l'autorité correspondante de l'Etat signalant ;

Considérant qu'en l'espèce, la commission nationale de l'informatique et des libertés a estimé nécessaire de communiquer, dans le cadre de la procédure contradictoire devant le Conseil d'Etat, des éléments d'information sur le signalement du requérant ;

Considérant que M. S., ressortissant français, a saisi la commission nationale de l'informatique et des libertés le 8 mars 2004 d'une demande d'effacement des données le concernant contenues dans le système informatique national du Système d'Information Schengen, en faisant notamment état de sa mobilisation au début des années 1990 au côté d'opposants tunisiens pour dénoncer les violations par le régime tunisien des droits de l'homme et des libertés fondamentales, et en indiquant " avoir fait manifestement l'objet d'une dénonciation calomnieuse des services de ce pays " ; que la commission nationale de l'informatique et des libertés, après avoir constaté que l'intéressé avait été signalé par les autorités allemandes, a saisi le 18 mai 2004 l'autorité de contrôle allemande chargée d'exercer un contrôle de la partie nationale du Système d'Information Schengen dans le cadre de la procédure de coordination prévue au paragraphe 2 de l'article 114 de la convention du 19 juin 1990 ; que l'autorité de contrôle allemande lui a répondu qu'" au terme de la vérification effectuée par le délégué régional compétent en matière de protection des données, (...) rien ne s'oppose, du point de vue du droit en matière de protection des données, au signalement de l'intéressé au Système d'Information Schengen " ; que, dans ces circonstances, et eu égard à l'ensemble des éléments d'information produits par le requérant, la commission nationale de l'informatique et des libertés, en se fondant sur cette seule réponse, sans demander communication des informations nécessaires au contrôle sollicité, pour refuser de poursuivre la procédure relative à la demande d'effacement du signalement de l'intéressé, a méconnu les stipulations des articles 106 et 114 de la convention du 19 juin 1990 ; qu'elle a ainsi entaché sa décision d'erreur de

droit ; que M. S. est fondé à en demander l'annulation ;

Considérant que l'annulation de la décision contestée implique que la commission nationale de l'informatique et des libertés reprenne la procédure de vérification relative au signalement de M. S., en " étroite coordination " avec l'autorité de contrôle allemande, aux fins d'aboutir soit au rejet de la demande en accord avec les autorités allemandes, soit à l'effacement des données litigieuses par les autorités allemandes, soit enfin, en cas de désaccord, à la saisine de l'autorité de contrôle commune mentionnée au paragraphe 3 de l'article 106 de la convention du 19 juin 1990 ;

Sur les conclusions tendant à l'application de l'article L. 761-1 du code de justice administrative :

Considérant qu'il y a lieu, dans les circonstances de l'espèce, de faire application de ces dispositions et de mettre à la charge de l'Etat la somme de 2 500 euros que demande M. S. au titre des frais exposés par lui et non compris dans les dépens ;

D E C I D E :

Article 1er : Il est donné acte du désistement des conclusions de la requête de M. S. tendant à la condamnation de l'Etat à lui verser une somme de 50 000 euros en réparation du préjudice subi.

Article 2 : Il n'y a pas lieu de statuer sur les conclusions de M. S. tendant à l'annulation de la décision de la commission nationale de l'informatique et des libertés en tant qu'elle a refusé communication des informations le concernant contenues dans le système informatique national du Système d'Information Schengen et s'est abstenue de prescrire l'effacement du signalement de

l'intéressé opéré à l'initiative des autorités françaises.

Article 3 : La décision de la commission nationale de l'informatique et des libertés du 12 octobre 2004 est annulée en tant qu'elle met un terme à la procédure d'effacement sans poursuite de l'examen du bien-fondé du signalement opéré par les autorités allemandes en étroite coordination avec celles-ci.

Article 4 : L'Etat versera une somme de 2 500 euros à M. S. au titre de l'article L. 761-1 du code de justice administrative.

Article 5 : La présente décision sera notifiée à M. Manar Mohamed S., à la commission nationale de l'informatique et des libertés et au ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire.

Décision n° 2004-499 DC du 29 juillet 2004



Décision n° 2004-499 DC

- Communiqué de presse
- Dossier complet et texte adopté sur le site de l'Assemblée nationale
- Dossier complet et texte adopté sur le site du Sénat
- Texte du projet de loi déposé
- Saisine par 60 députés
- Saisine par 60 sénateurs
- Observations du gouvernement
- Réplique députés
- Réplique sénateurs
- Dossier documentaire
- Législation consolidée avant décision
- Commentaire aux cahiers
- Version PDF de la décision
- Références doctrinales
- Décision n° 2004-499 DC du 29 juillet 2004

Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Le Conseil constitutionnel a été saisi, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le 20 juillet 2004, par M. Jean Marc AYRAULT, Mmes Patricia ADAM, Sylvie ANDRIEUX BACQUET, MM. Jean Marie AUBRON, Jean-Paul BACQUET, Gérard BAPT, Claude BARTOLONE, Jacques BASCOU, Christian BATAILLE, Jean-Claude BATEUX, Éric BESSON, Jean Louis BIANCO, Jean-Pierre BLAZY, Serge BLISKO, Patrick BLOCHE, Jean Claude BOIS, Maxime BONO, Augustin BONREPAUX, Jean Michel BOUCHERON, Pierre BOURGUIGNON, Mme Danielle BOUSQUET, MM. François BROTTES, Thierry CARCENAC, Christophe CARESCHE, Mme Martine CARILLON COUVREUR, MM. Laurent CATHALA, Jean Paul CHANTEGUET, Alain CLAEYS, Gilles COCQUEMPOT, Pierre COHEN, Mme Claude DARCIAUX, M. Michel DASSEUX, Mme Martine DAVID, MM. Marcel DEHOUX, Bernard DEROSIER, Marc DOLEZ, François DOSÉ, René DOSIÈRE, Julien DRAY, Tony DREYFUS, Pierre DUCOUT, Jean Pierre DUFAU, Jean-Paul DUPRÉ, Yves DURAND, Henri EMMANUELLI, Claude ÉVIN, Laurent FABIUS, Jacques FLOCH, Pierre FORGUES, Michel FRANÇAIX, Jean GAUBERT, Mmes Nathalie GAUTIER, Catherine GÉNISSON, MM. Jean GLAVANY, Gaétan GORCE, Alain GOURIOU, Mmes Elisabeth GUIGOU, Paulette GUINCHARD-KUNSTLER, M. David HABIB, Mme Danièle HOFFMAN RISPAL, MM. François HOLLANDE, Jean Louis IDIART, Mme Françoise IMBERT, MM. Serge JANQUIN, Armand JUNG, Jean-Pierre KUCHEIDA, Mme Conchita LACUEY, MM. Jérôme LAMBERT, François LAMY, Jack LANG, Jean LAUNAY, Jean-Yves LE BOUILLONNEC, Gilbert LE BRIS, Jean-Yves LE DÉAUT, Jean LE GARREC, Jean-Marie LE GUEN, Bruno LE ROUX, Mme Marylise LEBRANCHU, MM. Michel LEFAIT, Patrick LEMASLE, Guy LENGAGNE, Mme Annick LEPETIT, MM. Jean Claude LEROY, Michel LIEBGOTT, Mme Martine LIGNIÈRES CASSOU, MM. François LONCLE, Bernard MADRELLE, Christophe MASSE, Didier MATHUS, Kléber MESQUIDA, Jean MICHEL, Didier MIGAUD, Mme Hélène MIGNON, MM. Arnaud MONTEBOURG, Henri NAYROU, Alain NÉRI, Mme Marie-Renée OGET, MM. Christian PAUL, Germinal PEIRO, Mmes Marie-Françoise PÉROL DUMONT, Geneviève PERRIN GAILLARD, MM. Jean-Jack QUEYRANNE, Paul QUILÈS, Alain RODET, Bernard ROMAN, René ROUQUET, Mmes Ségolène ROYAL, Odile SAUGUES, MM. Henri SICRE, Dominique STRAUSS KAHN, Pascal TERRASSE, Daniel VAILLANT, André VALLINI, Manuel VALLS, Michel VERGNIER, Alain VIDALIES, Jean Claude VIOLLET, Philippe VUILQUE, Jean-Pierre DEFONTAINE, Paul GIACOBBI, Joël GIRAUD, Simon RENUCCI, Mme Chantal ROBIN RODRIGO, M. Roger-Gérard SCHWARTZENBERG et Mme Christiane TAUBIRA, députés ;

et le même jour, par M. Claude ESTIER, Mme Michèle ANDRÉ, MM. Bernard ANGELS, Bertrand AUBAN, Robert BADINTER, Jean Pierre BEL, Mme Maryse BERGÉ LAVIGNE, M. Jean BESSON, Mme Marie-Christine BLANDIN, M. Didier BOULAUD, Mmes Yolande BOYER, Claire-Lise CAMPION, MM. Jean-Louis CARRÈRE, Bernard CAZEAU, Mme Monique CERISIER-ben GUIGA, MM. Gilbert CHABROUX, Gérard COLLOMB, Raymond COURRIÈRE, Yves DAUGE, Marcel DEBARGE, Jean Pierre DEMERLIAT, Claude DOMEIZEL, Michel DREYFUS SCHMIDT, Bernard DUSSAUT, Bernard FRIMAT, Charles GAUTIER, Jean Pierre GODEFROY, Jean-Noël GUÉRINI, Mme Odette HERVIAUX, MM. André LABARRÈRE, Serge LAGAUCHE, Louis LE PENSEC, André LEJEUNE, Jacques MAHÉAS, Jean-Yves MANO, François MARC, Jean Pierre MASSERET, Pierre MAUROY, Louis MERMAZ, Gérard MIQUEL, Michel MOREIGNE, Jean-Claude PEYRONNET, Jean François PICHERAL, Bernard PIRAS, Jean Pierre PLANCADE, Mmes Danièle POURTAUD, Gisèle PRINTZ, MM.

Daniel RAOUL, Daniel REINER, Roger RINCHET, Gérard ROUJAS, Claude SAUNIER, Michel SERGENT, René Pierre SIGNÉ, Jean Pierre SUEUR, Simon SUTOUR, Michel TESTON, Jean Marc TODESCHINI, Pierre-Yvon TRÉMEL, André VANTOMME, André VÉZINHET et Marcel VIDAL, sénateurs ;
LE CONSEIL CONSTITUTIONNEL,

Vu la Constitution ;
Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ;
Vu le Traité instituant la Communauté européenne ;
Vu le Traité sur l'Union européenne ;
Vu la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;
Vu le code pénal ;
Vu le code de la propriété intellectuelle ;
Vu le code des postes et des communications électroniques ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
Vu la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, en son article 8 ;
Vu les observations du Gouvernement, enregistrées le 23 juillet 2004 ;
Vu les observations en réplique présentées par les députés auteurs de la première saisine, enregistrées le 28 juillet 2004 ;
Vu les observations en réplique présentées par les sénateurs auteurs de la seconde saisine, enregistrées le 28 juillet 2004 ;
Le rapporteur ayant été entendu ;

1. Considérant que les auteurs des deux saisines défèrent au Conseil constitutionnel la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; qu'ils dénoncent son inintelligibilité et mettent en cause les articles 8, 9, 21, 22 et 26 de la loi du 6 janvier 1978 tels qu'ils résultent des articles 2 à 4 de la loi déférée ;
- SUR LES NORMES CONSTITUTIONNELLES APPLICABLES À LA LOI DÉFÉRÉE ;
2. Considérant, en premier lieu, qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression » ; que la liberté proclamée par cet article implique le respect de la vie privée ;
3. Considérant, en deuxième lieu, qu'il est à tout moment loisible au législateur, statuant dans le domaine de sa compétence, de modifier des textes antérieurs ou d'abroger ceux-ci en leur substituant, le cas échéant, d'autres dispositions, dès lors que, ce faisant, il ne prive pas

de garanties légales des exigences constitutionnelles ;

4. Considérant, en troisième lieu, qu'il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il lui appartient d'assurer la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles liées notamment à la sauvegarde de l'ordre public ;

- SUR LE NOUVEL ARTICLE 8 DE LA LOI DU 6 JANVIER 1978 :

5. Considérant que l'article 8 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déferée, dispose en son I : « Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » ; que le 5° du II du même article 8 prévoit que, dans la mesure où la finalité du traitement l'exige, cette interdiction ne s'applique pas aux « traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice » ;

6. Considérant que les auteurs des saisines soutiennent que cette dernière disposition porte atteinte au respect de la vie privée ;

7. Considérant qu'aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'États qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences » ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ; qu'en l'absence d'une telle disposition, il n'appartient qu'au juge communautaire, saisi le cas échéant à titre préjudiciel, de contrôler le respect par une directive communautaire tant des compétences définies par les traités que des droits fondamentaux garantis par l'article 6 du traité sur l'Union européenne ;

8. Considérant que les dispositions critiquées se bornent à tirer les conséquences nécessaires des dispositions inconditionnelles et précises du e) du 2 de l'article 8 de la directive 95/46/CE du 24 octobre 1995 susvisée sur lesquelles il n'appartient pas au Conseil constitutionnel de se prononcer ; que, par suite, le grief tiré de l'atteinte au respect de la vie privée ne peut être utilement présenté devant lui ;

- SUR LE NOUVEL ARTICLE 9 DE LA LOI DU 6 JANVIER 1978 :

9. Considérant que l'article 9 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déferée, dispose : « Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en place que par : ... - 3° Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi ; - 4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits » ;

10. Considérant que, selon les auteurs des saisines, ces dispositions portent atteinte au respect de la vie privée et sont entachées d'incompétence négative ;

- . En ce qui concerne le 3° :
11. Considérant que le 3° de l'article 9 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déferée, permettrait à une personne morale de droit privé, mandatée par plusieurs autres personnes morales estimant avoir été victimes ou être susceptibles d'être victimes d'agissements passibles de sanctions pénales, de rassembler un grand nombre d'informations nominatives portant sur des infractions, condamnations et mesures de sûreté ; qu'en raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en oeuvre et de la nature des informations traitées, le 3° du nouvel article 9 de la loi du 6 janvier 1978 pourrait affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution ;
12. Considérant que, s'agissant de l'objet et des conditions du mandat en cause, la disposition critiquée n'apporte pas ces précisions ; qu'elle est ambiguë quant aux infractions auxquelles s'applique le terme de « fraude » ; qu'elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction ; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations ; qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés ; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures ; que, par suite, le 3° du nouvel article 9 de la loi du 6 janvier 1978 est entaché d'incompétence négative ;
- . En ce qui concerne le 4° :
13. Considérant que la possibilité ouverte par la disposition contestée donne la possibilité aux sociétés de perception et de gestion des droits d'auteur et de droits voisins, mentionnées à l'article L. 321 1 du code de la propriété intellectuelle, ainsi qu'aux organismes de défense professionnelle, mentionnés à l'article L. 331 1 du même code, de mettre en oeuvre des traitements portant sur des données relatives à des infractions, condamnations ou mesures de sûreté ; qu'elle tend à lutter contre les nouvelles pratiques de contrefaçon qui se développent sur le réseau Internet ; qu'elle répond ainsi à l'objectif d'intérêt général qui s'attache à la sauvegarde de la propriété intellectuelle et de la création culturelle ; que les données ainsi recueillies ne pourront, en vertu de l'article L. 34-1 du code des postes et des communications électroniques, acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire et par rapprochement avec des informations dont la durée de conservation est limitée à un an ; que la création des traitements en cause est subordonnée à l'autorisation de la Commission nationale de l'informatique et des libertés en application du 3° du I de l'article 25 nouveau de la loi du 6 janvier 1978 ; que, compte tenu de l'ensemble de ces garanties et eu égard à l'objectif poursuivi, la disposition contestée est de nature à assurer, entre le respect de la vie privée et les autres droits et libertés, une conciliation qui n'est pas manifestement déséquilibrée ;
- . En ce qui concerne l'ensemble de l'article 9 :
14. Considérant que le nouvel article 9 de la loi du 6 janvier 1978, tel qu'il résulte de la déclaration d'inconstitutionnalité prononcée en vertu

de ce qui précède, ne saurait être interprété comme privant d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victime ; que, sous cette réserve, il n'est pas contraire à la Constitution ;

- SUR LE NOUVEL ARTICLE 21 DE LA LOI DU 6 JANVIER 1978 ;

15. Considérant qu'en vertu du dernier alinéa de l'article 21 de la loi du 6 janvier 1978, dans sa rédaction issue de l'article 3 de la loi déferée, les personnes interrogées dans le cadre des vérifications faites par la Commission nationale de l'informatique et des libertés sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions « sauf dans les cas où elles sont astreintes au secret professionnel » ;

16. Considérant que, selon les requérants, cette référence au secret professionnel constitue « un recul quant aux garanties apportées aux exigences constitutionnelles applicables en la matière » ; qu'ils font valoir que « dans la loi de 1978, il n'était pas possible d'opposer un tel secret aux agents de la CNIL » et qu'« une telle restriction déséquilibre manifestement le régime de protection de la vie privée et de la liberté individuelle des personnes dont les données personnelles ont fait l'objet d'un traitement » ;

17. Considérant que, dans le silence des dispositions de la loi du 6 janvier 1978 antérieures à la loi déferée, les personnes interrogées par la Commission nationale de l'informatique et des libertés étaient déjà soumises au secret professionnel ; que, dès lors, le grief manque en fait ;

18. Considérant, au demeurant, que l'invocation injustifiée du secret professionnel pourrait constituer une entrave passible des peines prévues par l'article 51 nouveau de la loi du 6 janvier 1978 ;

- SUR LE NOUVEL ARTICLE 22 DE LA LOI DU 6 JANVIER 1978 ;

19. Considérant qu'aux termes du premier alinéa du III de l'article 22 de la loi du 6 janvier 1978, dans sa rédaction issue de l'article 4 de la loi déferée : « Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé » ;

20. Considérant que, selon les requérants, « ce correspondant ne bénéficie pas, à la lettre, des garanties d'indépendance indispensables » ; qu'ils considèrent, dès lors, qu'« en prévoyant, au titre d'une simplification toujours souhaitable, un amoindrissement des mécanismes de contrôle, le législateur a privé de garantie légale le droit à la vie privée et à la liberté individuelle » ;

21. Considérant, en premier lieu, que le fait de désigner un correspondant à la protection des données à caractère personnel n'a d'autre effet que d'exonérer les traitements des formalités de déclaration auprès de la Commission nationale de l'informatique et des libertés ; que cette circonstance ne les soustrait pas aux autres obligations résultant de la loi déferée, dont le non respect demeure passible des sanctions qu'elle prévoit ; que cet allègement de la procédure n'est pas possible lorsque des transferts de données à destination d'un État non membre de la Communauté européenne sont envisagés ; qu'en outre, il ne concerne pas les traitements soumis à autorisation ;

22. Considérant, en second lieu, que le correspondant, dont l'identité est notifiée à la Commission nationale de l'informatique et des libertés

et portée à la connaissance des instances représentatives du personnel, doit bénéficier, en vertu de la loi, « des qualifications requises pour exercer ses missions » ; qu'il tient la liste des traitements à la disposition de toute personne en faisant la demande ; qu'il ne peut faire l'objet d'aucune sanction de la part de son employeur du fait des responsabilités qui lui sont confiées dans l'exercice de sa mission ; qu'il peut saisir la Commission nationale de l'informatique et des libertés, le cas échéant, des difficultés qu'il rencontre ;

23. Considérant que, compte tenu de l'ensemble des précautions ainsi prises, s'agissant en particulier de la qualification, du rôle et de l'indépendance du correspondant, la dispense de déclaration résultant de sa désignation ne prive de garanties légales aucune exigence constitutionnelle ;

- SUR LE NOUVEL ARTICLE 26 DE LA LOI DU 6 JANVIER 1978 :

24. Considérant qu'aux termes du I de l'article 26 de la loi du 6 janvier 1978, dans sa rédaction issue de l'article 4 de la loi déferée : « Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État et : - 1° Qui intéressent la sûreté de l'État, la défense ou la sécurité publique ; - 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, ou l'exécution des condamnations pénales ou des mesures de sûreté. - L'avis de la commission est publié avec l'arrêté autorisant le traitement » ;

25. Considérant que, selon les requérants, ces dispositions marquent « un des reculs les plus manifestes opérés par cette loi quant au niveau des garanties légales constitutionnellement exigées puisque aujourd'hui un tel traitement requiert un avis favorable de la CNIL » ; qu'ils considèrent que cette évolution crée, « au regard de l'article 2 de la Déclaration de 1789 et de la liberté individuelle », une « situation constitutionnellement préjudiciable » ;

26. Considérant que le I de l'article 26 de la loi du 6 janvier 1978 est relatif à la création des seuls traitements intéressant la sauvegarde de l'ordre public et ne comportant pas de données sensibles au sens du I de son article 8 ; qu'il se borne à substituer à un avis conforme du Conseil d'État en cas d'avis défavorable de la Commission nationale de l'informatique et des libertés un arrêté ministériel pris après avis motivé et publié de la Commission ; que le législateur a prévu que l'avis de la Commission serait publié concomitamment à l'arrêté autorisant le traitement ;

27. Considérant, dans ces conditions, que les dispositions critiquées, qui ne privent pas de garanties légales le droit au respect de la vie privée, ne sont contraires à aucun principe ni à aucune règle de valeur constitutionnelle ;

- SUR L'OBJECTIF DE VALEUR CONSTITUTIONNELLE D'INTELLIGIBILITÉ ET D'ACCESSIBILITÉ DE LA LOI :

28. Considérant que, selon les requérants, « l'ensemble du texte souffre d'une opacité qui... ne peut que paraître contradictoire avec l'objectif d'intelligibilité et de clarté de la loi » ;

29. Considérant qu'il incombe au législateur d'exercer pleinement la compétence que lui confie la Constitution et, en particulier, son article 34 ; qu'à cet égard, l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, qui découle des articles 4, 5, 6 et 16 de la Déclaration de 1789, lui impose d'adopter des dispositions suffisamment précises et des formules non équivoques ;

30. Considérant que, si la loi déferée refond la législation relative à la protection des données personnelles, c'est en vue d'adapter cette

législation à l'évolution des données techniques et des pratiques, ainsi que pour tirer les conséquences d'une directive communautaire ; qu'elle définit de façon précise les nouvelles règles de procédure et de fond applicables ;
31. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune question de conformité à la Constitution,

Décide :

Article premier.- Est déclaré contraire à la Constitution le 3° de l'article 9 de la loi susvisée du 6 janvier 1978, dans sa rédaction issue de l'article 2 de la loi déferée.

Article 2.- Ne sont pas contraires à la Constitution les articles 8, 21, 22 et 26 nouveaux de la loi du 6 janvier 1978, ainsi que, sous la réserve énoncée au considérant 14, le surplus de son article 9.

Article 3.- La présente décision sera publiée au Journal officiel de la République française.
Délibéré par le Conseil constitutionnel dans sa séance du 29 juillet 2004, où siégeaient : M. Pierre MAZEAUD, Président, MM. Jean Claude COLLIARD, Olivier DUTHELLET de LAMOTHE, Mme Jacqueline de GUILLENCHMIDT, MM. Pierre JOXE et Jean-Louis PEZANT, Mme Dominique SCHNAPPER, M. Pierre STEINMETZ et Mme Simone VEIL.

Publication Journal officiel du 7 août 2004, p. 14087

Délibération n°2006-174 du 28 juin 2006 prononçant une sanction pécuniaire à l'encontre du Crédit Lyonnais (LCL)

28 Juin 2006 - Thème(s) : Banque - Finance

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex Türk, président ;

Etant aussi présents M. Guy Rosier, vice-président délégué, M. François Giquel, vice-président, M. Hubert Bouchet, membre, Mlle Anne Debet, membre, M. Bernard Peyrat, membre ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction antérieure à la loi du 6 août 2004 ;

Vu la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu les délibérations n° 2006-032 et n° 2006-033 adoptées par la CNIL le 21 février 2006 ;

Vu les saisines n° 04018295, n° 05006569, n° 05009907 et n° 05015327

Vu le rapport de M. Philippe Nogrix, commissaire, notifié le 18 mai 2006 au Crédit Lyonnais et les observations en réponse reçues le 14 juin 2006.

Après avoir entendu, lors de la réunion du 28 juin 2006, M. Philippe Nogrix, commissaire, en son rapport et Mme Pascale Compagnie, commissaire du

Gouvernement, en ses observations.

Après avoir entendu, lors de la réunion du 28 juin 2006, les observations orales de MM. Hubert Massiet du Biest, Responsable de la Conformité LCL, Gérard Wissing, Direction des Affaires Juridiques et Michel Corbion, Service Relations Clientèle, ceux-ci ayant pris la parole en dernier.

Constate les faits suivants :

1. La Commission a été saisie d'une plainte le 15 novembre 2004 (n° 04018295) concernant le retard pris par le Crédit Lyonnais dans la mainlevée d'une inscription au FICP effectuée le 28 février 2002. A l'appui de sa demande, le requérant joignait la copie d'avis d'opération indiquant que l'incident de paiement ayant justifié son inscription au FICP avait été régularisé le 16 septembre 2004. Le 10 décembre 2004, les services de la Banque de France ont confirmé à la Commission que le requérant était encore inscrit au FICP.

a. Dans le cadre de l'instruction de la plainte, la CNIL a demandé au Crédit Lyonnais par courrier daté du 15 décembre 2004 de lui indiquer la nature exacte des incidents de paiement caractérisés ayant justifié l'inscription au FICP ainsi que les raisons pour lesquelles il n'avait pas été procédé à la mainlevée de cette inscription au moment de la régularisation de l'incident de paiement.

Par courrier du 16 février 2005, le Crédit Lyonnais a indiqué à la CNIL, sans autre précision, la survenance « d'anomalies » qui auraient justifié l'inscription au FICP et a observé que les incidents de paiement concernant le requérant étaient régularisés sans être en mesure d'indiquer à quelle date la mainlevée de l'inscription avait été effectuée, motif pris qu'aucune opération d'archivage ou d'historisation n'était effectuée concernant cette information dans leurs systèmes informatiques. Le Crédit Lyonnais a néanmoins précisé qu'une interrogation du FICP, sans pour autant joindre la copie de ce document, attestait de l'absence d'inscription du requérant le 15 décembre 2004.

Observant que le Crédit Lyonnais n'avait pas répondu aux questions posées dans son précédent courrier, la CNIL lui a adressé un second courrier de demande de compléments en date du 24 mars 2005 réitérant les requêtes formulées dans son courrier du 15 décembre 2004 et s'étonnant de l'absence d'informations, dans les systèmes informatiques du Crédit Lyonnais, concernant tant l'historique des incidents de paiement que leur régularisation.

Par courrier du 9 mai 2005, le Crédit Lyonnais a indiqué ne pas être en mesure d'apporter les informations complémentaires sollicitées par la CNIL.

b. Conformément à la décision n° 2005-100C du 22 novembre 2005, les services de la CNIL ont procédé le 1er décembre 2005 à une mission de vérification sur

place auprès de l'agence bancaire teneur du compte du requérant ; ils ont constaté qu'il était impossible d'obtenir sur place les informations requise le compte ayant été fermé et aucune donnée informatique relative aux incidents n'étant accessible depuis l'agence.

En janvier 2006, les services de la CNIL ont poursuivi leurs investigations en se rendant dans un centre informatique du Crédit Lyonnais afin de pouvoir consulter, notamment, les archives informatiques de la banque et se sont donc rapprochés, de façon informelle, des services du Crédit Lyonnais afin de connaître les coordonnées exactes de leurs centres informatiques.

En réponse à cette demande, le Crédit Lyonnais a adressé le 16 janvier 2006 un courrier au Président de la CNIL rappelant les échanges de courriers précités et indiquant que les incidents de paiement caractérisés « remontent à avril 2002, le compte a été soldé par perte le 16/09/04, et notre requête du 15/12/04 mentionne l'absence d'inscription du FICP à cette date, la radiation étant donc antérieure à cette date ».

Dans ce courrier, le Crédit Lyonnais n'avait cependant pas répondu à la demande de la CNIL concernant la localisation des moyens informatiques permettant de poursuivre la mission de vérification sur place ; ce n'est qu'après de nombreux échanges effectués par téléphone, télécopies et courriers électroniques, que cette information a enfin été communiquée à la CNIL le 20 janvier 2006.

Le 25 janvier 2006 une seconde mission de contrôle a été, en conséquence, diligentée auprès des services informatiques du Crédit Lyonnais. Cette mission s'est poursuivie le 3 février 2006 dans les locaux du Crédit Lyonnais afin de consulter le dossier papier du requérant qui n'était pas disponible avant cette date raison des délais de désarchivage du dossier.

Il est ressorti de l'ensemble des investigations menées par les services de la Commission que :

- Une trace informatique des inscriptions au FICP ainsi que de la régularisation des incidents de paiement était bien conservée dans une application informatique interne au Crédit Lyonnais dénommée « FICL ». Dans cette application « FICL », la délégation de la CNIL a ainsi pu retrouver la date de l'incident de paiement caractérisé ainsi que la date de déclaration de cet incident à la Banque de France qui remontaient à février 2002. Pourtant, par courriers des 16 février, 9 mai 2005 et 16 janvier 2006, le Crédit Lyonnais avait soutenu ne disposer d'aucun élément concernant l'archivage ou l'historisation d'informations permettant de retracer les dates d'inscription et de mainlevée d'une personne dans le FICP.

- Les services de la CNIL ont eu connaissance, lors des missions de contrôle, de la raison exacte pour laquelle la mainlevée de l'inscription au FICP du requérant avait été effectuée tardivement. Un incident technique survenu dans les systèmes informatiques du Crédit Lyonnais, à la suite du changement d'un prestataire, a empêché le défilement automatique de certains clients ayant régularisé leur incident de paiement. Les difficultés rencontrées par le requérant, loin d'être isolées, ont donc manifestement été subies par d'autres clients. Ces dysfonctionnements techniques, mentionnés dans des documents internes du Crédit Lyonnais en date

des 24 et 25 janvier 2005, n'ont jamais été communiqués aux services de la CNIL.

Ces faits constituaient par conséquent un manquement aux obligations découlant de la loi du 6 janvier 1978 modifiée. Celle-ci prévoit, en effet :

- dans son article 11-2°-c que la CNIL reçoit les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel.

- dans son article 21 alinéa 2 que « les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche ».

- dans son article 51 « qu'est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés : 1° en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités ; 2° en dissimulant [des] documents ou renseignements, ou en les faisant disparaître ; 3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible ».

Si le principe du droit à l'oubli évoqué par le Crédit Lyonnais dans plusieurs de ses correspondances peut justifier la mise en œuvre d'une politique de restriction d'accès, par le réseau commercial, à l'information relative à l'inscription d'un client dans les fichiers de la Banque de France, celui-ci ne fait nullement obstacle à la conservation, dans une base d'archives à accès restreint, de ces informations.

2. La Commission a également été saisie de trois plaintes les 12 mai 2005 (n° 05006569), 21 juillet 2005 (n° 05009907) et le 1er août 2005 (n° 05015327) concernant l'inscription de requérants par le Crédit Lyonnais les 12 janvier, 16 août 2004, 21 janvier et 17 juin 2005 au fichier des retraits « CB » mis en œuvre par la Banque de France.

Dans le cadre de l'instruction de ces plaintes, la CNIL a demandé au Crédit Lyonnais par courriers datés des 27 juillet, 18 août, 1er décembre, 15 décembre, 26 décembre 2005 et 13 février 2006 de lui indiquer notamment la nature exacte des incidents de fonctionnement des comptes bancaires des requérants résultant de l'usage d'une carte qui ont entraîné leur inscription fichier des retraits « CB ».

Le Crédit Lyonnais n'a apporté aucune suite à ces demandes et, par courriers reçus le 19 janvier, 27 janvier et 17 février 2006, a indiqué à la Commission que : « le secret professionnel auquel nous sommes soumis, et qui est assorti de sanctions pénales, ne nous permet pas de détailler la nature des incidents constatés ».

Or ces faits constituent un manquement aux obligations découlant de la loi du 6 janvier 1978 modifiée ; il résulte, en effet :

- de l'article 21 alinéa 2 de ce texte que « les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche ».

- de l'article 11-2°-c de ladite loi que la CNIL reçoit les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel.

Si les données à caractère personnel concernant un client bancaire sont effectivement protégées par le secret professionnel en application des dispositions de l'article L 511-33 du code monétaire et financier, force est de constater que ce secret a pour vocation de protéger le titulaire du compte lui-même.

Ainsi, dès lors que le titulaire d'un compte bancaire adresse à la CNIL un courrier écrit par lequel il dépose une réclamation auprès de la CNIL et lui demande de procéder à des vérifications auprès d'un responsable de traitement, opposer à la CNIL l'existence du secret bancaire, c'est l'opposer au titulaire des comptes qu'elle a en charge de protéger, ce qui viderait cette disposition de sa raison d'être.

Le refus opposé par le Crédit Lyonnais aux demandes formulées par la CNIL dans ses différents courriers, outre que celui-ci a été formulé de façon tardive, est donc susceptible de relever l'article 51 de la loi du 6 janvier 1978 modifiée qui dispose que : « Est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés : 1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ; 2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ».

3. Au regard de ce qui précède, la CNIL a, par délibérations adoptées le 21 février 2006, mis en demeure le Crédit Lyonnais de :

- justifier les différences relevées par la CNIL entre les informations communiquées par le Crédit Lyonnais dans ses courriers des 16 février, 9 mai 2005 et 16 janvier 2006 et les informations dont la CNIL a pris connaissance lors de ses différentes missions de vérification sur place ;

- apporter tout élément de fait permettant de considérer qu'il n'y a pas eu de dissimulation de preuve ou de communication à la CNIL, dans le cadre de l'instruction de la plainte du requérant de novembre 2004 à janvier 2006, d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les demandes ont été formulées par la CNIL notamment dans ses courriers des 15 décembre 2004 et 25 mars 2005 ;

- répondre aux demandes de complément formulées par la CNIL dans ses courriers des 27 juillet, 18 août, 1er décembre, 15 décembre, 26 décembre 2005 et 13 février 2006 et d'apporter toute garantie sur la régularité de l'inscription des requérants, au regard de l'ensemble des dispositions de la loi du 6 janvier 1978

modifiée, au fichier des retraits « CB » mis en œuvre par la Banque de France.

En réponse aux mises en demeure de la CNIL, le Crédit Lyonnais a adressé, le 10 mars 2006, plusieurs courriers.

a. S'agissant de la saisine n° 04018295, le Crédit Lyonnais a indiqué que : « Il est certain (...) que les différents éléments de réponse qui vous ont été apportés par nos courriers des 16 février, 9 mai 2005 et 16 janvier 2006 mettent en exergue certaines différences au regard des investigations menées sur place par vos collaborateurs (...) La mission que vous avez conduite (...) met en lumière plusieurs points parmi lesquels nous relevons le circuit et les modalités de traitement de ces demandes s'organisant dans des conditions qui manifestement sont encore perfectibles chez nous (...) Il apparaît que les informations que vous recherchez sur les dates d'inscription et de radiation du FICP n'ont pu être fournies à cause d'un archivage protégé qui n'est accessible qu'à certains collaborateurs insuffisamment identifiés. Les modalités d'accès à ces informations doivent donc être redéfinies, ainsi que les rôles des différents intervenants afin d'assurer une meilleure qualité dans les investigations effectuées par le Crédit Lyonnais. Nous mettons donc en chantier les modifications structurelles nécessaires dans ce but, car le dispositif adopté par notre établissement pour accompagner la mission de la CNIL a permis d'apporter les informations souhaitées ».

Tout en tenant compte de l'explication fournie par le Crédit Lyonnais ainsi que des engagements significatifs visés dans son courrier, on est en droit de s'interroger sur les conditions exactes dans lesquelles des investigations ont été menées par les services du Crédit Lyonnais lorsque ceux-ci ont été sollicités par les services de la CNIL dans le cadre de l'instruction de la plainte du requérant (courriers des 15 décembre 2004 et 24 mars 2005).

En effet, il ressort des courriers électroniques internes figurant dans le dossier papier du requérant dont la CNIL a pris connaissance lors de sa mission de contrôle du 3 février 2006 que, dès le 12 avril 2005, les services du Crédit Lyonnais faisaient référence, dans leurs échanges, à la procédure à mettre en œuvre pour accéder à l'application « FICL ». De même, un message électronique daté du 24 janvier 2005 évoquait des dysfonctionnements techniques liés à l'absence de mainlevée de l'inscription au FICP du requérant or bien que connus dès cette date, ces dysfonctionnements n'ont pas été portés à la connaissance de la CNIL.

b. S'agissant des saisines n° 05015327, 05006569 et 05009907 concernant l'inscription de requérants au fichier des retraits « CB » mis en œuvre par la Banque de France, le Crédit Lyonnais a accepté de communiquer à la CNIL les informations qui lui avaient été demandées, conformément aux dispositions des articles 11-2°-c, 21 al. 2 et 51 de la loi du 6 janvier 1978 modifiée.

Il convient de rappeler au préalable que le traitement dénommé « centralisation des retraits de cartes bancaires » a été créé par un arrêté du conseil général de la Banque de France du 16 juillet 1987. Il est inclus, sur le plan technique, dans le Fichier central des chèques (FCC) mais il répond, sur le plan juridique, à des règles de fonctionnement spécifiques. L'article 2.1 de l'arrêté précité dispose en particulier que : « Font l'objet d'une déclaration à la Banque de France les décisions de retraits de cartes bancaires « CB » prises par les émetteurs à la suite d'incidents de fonctionnement du compte qui résultent directement de l'usage

desdites cartes ».

Ainsi, l'inscription d'une personne au fichier des retraits « CB » est régulière si elle est liée à des incidents de fonctionnement du compte qui résultent directement de l'usage desdites cartes, nonobstant la faculté réservée à chaque établissement de crédit de prévoir contractuellement des conditions plus larges de blocage de l'utilisation d'une carte bancaire : ce blocage devant être strictement limité à un blocage interne à l'établissement de crédit concerné et non mutualisé à l'ensemble des établissements ayant accès au fichier mis en œuvre par la Banque de France.

b1. S'agissant de la saisine n° 05010327, le Crédit Lyonnais a apporté à la CNIL les précisions suivantes : « Mme xxx est titulaire d'un compte ouvert dans les livres de notre agence 2861 à Gardanne, sous le n° 11570F. La carte bancaire de Madame xxx (validité septembre 2004) a fait l'objet le 20 juin 2003 d'une mesure de blocage (interne au Crédit Lyonnais) en raison de l'émission de chèques sans provision. Elle n'a plus été utilisée après cette date. Le 12 janvier 2004, le compte étant débiteur et l'échéance d'un crédit permanent n'ayant pas été réglée, le dossier de Madame xxx a été transmis au secteur recouvrement amiable ce qui a entraîné, conformément aux procédures internes applicables aux cartes en cours de validité, la mise en « opposition usage abusif » qui déclenche automatiquement une déclaration au FCC ».

Cependant le Crédit Lyonnais n'a apporté aucun élément précis et justifié par des documents comptables attestant de l'existence d'incidents de fonctionnement du compte qui résultaient directement de l'usage de la carte bancaire de la requérante ; il a précisé au contraire que les cartes bancaires de la requérante avaient été bloquées dès le mois de juin 2003. Cette dernière a d'ailleurs indiqué les avoir retournées, en juillet 2003, à son agence.

En outre, le Crédit Lyonnais a fait état, pour justifier l'inscription de la requérante au fichier des retraits « CB », de l'émission de chèques sans provision ainsi que d'une échéance de crédit permanent non réglée. Ces deux incidents pouvaient justifier, le cas échéant, l'inscription de la requérante au Fichier central des chèques (FCC) ainsi qu'au FICP mais en aucune manière dans les fichiers des retraits « CB ».

Enfin, le Crédit Lyonnais a indiqué que ses procédures internes prévoyaient l'inscription systématique au fichier des retraits « CB » de l'ensemble des clients en situation de recouvrement. Cette procédure n'est manifestement pas conforme aux dispositions de l'arrêté du conseil général de la Banque de France du 16 juillet 1987, notamment son article 2.1.

b2. S'agissant de la saisine n° 05006569, il est ressorti des éléments communiqués par le Crédit Lyonnais par courrier du 10 mars 2006 que la requérante : « est notamment titulaire d'un compte joint (...) Le 27 avril 2004, ce compte a fait l'objet d'un blocage en exécution d'une réquisition judiciaire sur commission rogatoire (...) Les échéances des prêts en cours ne pouvant plus être prélevées, le dossier a été transmis à notre service de recouvrement amiable et parallèlement une inscription du retrait de la carte bancaire liée à ce compte a été opérée le 16 août 2004 auprès de la Banque de France ».

Or le Crédit Lyonnais n'a apporté, dans cette affaire, aucun élément précis et justifié par des documents comptables attestant de l'existence d'incidents de fonctionnement du compte qui résultaient directement de l'usage de la carte bancaire de la requérante.

b3. S'agissant enfin de la saisine n° 05009907, il est ressorti des éléments communiqués par le Crédit Lyonnais par courrier du 10 mars 2006 que le requérant : « est titulaire d'un compte ouvert dans les livres de notre agence 7600 à Orléans (...) L'inscription au FCC du 21 janvier 2005 a été initiée à raison de la position débitrice du compte de 668,70 €. L'inscription au FCC du 17 juin 2005 a été initiée alors que le compte présentait un solde créditeur de 39,85 € en raison d'échéances impayées en souffrance pour un montant de 123,13 € et alors qu'il s'agissait d'un second usage abusif (l'inscription du 21 janvier 2005) ».

Là encore, le Crédit Lyonnais n'a apporté aucun élément précis et justifié par des documents comptables attestant de l'existence d'incidents de fonctionnement du compte qui résultaient directement de l'usage de la carte bancaire du requérant. En outre, les deux inscriptions du requérant au volet « CB » du FCC étaient toujours effectives le 31 mars 2006.

Il apparaît que, dans l'ensemble de ses réponses, le Crédit Lyonnais n'a donc pas apporté des éléments comptables précis et justifiés sur la nature des incidents de fonctionnement des comptes des requérants liés à l'utilisation d'une carte bancaire (comme le lui avait demandé tout au long de la procédure dans les courriers en date des 27 juillet, 18 août, 1er décembre, 15 décembre, 26 décembre 2005 et 13 février 2006).

Au regard de ce qui précède la CNIL a considéré que le Crédit Lyonnais n'avait pas respecté les conditions d'inscription au fichier des retraits « CB » visées dans l'arrêté du conseil général de la Banque de France du 16 juillet 1987 et que les inscriptions des requérants, toujours en cours pour l'un d'entre eux, n'étaient pas justifiées.

C'est, dans ces conditions, que le rapporteur, au regard des faits précités, a notifié au Crédit Lyonnais le 18 mai 2006 une proposition de sanction.

4- a. Aux termes du courrier adressé par le Crédit Lyonnais le 14 juin 2006 et des observations orales formulées par ses représentants lors de la réunion du 28 juin 2006, le Crédit Lyonnais a fait valoir qu'il avait non seulement répondu à l'ensemble des demandes de la CNIL mais qu'il avait toujours cherché à le faire « le plus efficacement possible en fournissant les renseignements accessibles ».

Or, la CNIL souligne que le Crédit Lyonnais n'a apporté aucune explication sur les raisons qui l'ont conduit à ne pas lui communiquer, pendant près d'un an, les informations qu'elle lui avait demandées, notamment dans ses courriers des 15 décembre 2004 et 25 mars 2005 et alors que ces informations étaient manifestement connues des services de cette banque, comme l'attestent les éléments retrouvés par la CNIL lors des missions de contrôle réalisées les 25 janvier et 3 février 2006.

Rappelant :

- l'article 11-2°-c de la loi du 6 janvier 1978 modifiée le 6 août 2004 prévoyant que la CNIL reçoit les plaintes relative à la mise en œuvre des traitements de données à caractère personnel.

- l'article 21, alinéa 2 de ladite loi disposant par ailleurs que « les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche ».

- l'article 51 de la même loi stipulant « qu'est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés : 2° en dissimulant [des] documents ou renseignements, ou en les faisant disparaître ; 3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible ».

la Commission estime que le Crédit Lyonnais ne s'est pas conformé à la mise en demeure du 21 février 2006 qui lui demandait d'apporter tout élément de fait permettant de considérer qu'il n'y a pas eu de dissimulation de preuve ou de communication à la CNIL, dans le cadre de l'instruction de la plainte du requérant de novembre 2004 à janvier 2006, d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les demandes ont été formulées par la CNIL notamment dans ses courriers des 15 décembre 2004 et 25 mars 2005.

- b. La Commission observe par ailleurs que le Crédit Lyonnais n'a apporté, ni dans son courrier d'observations adressé le 14 juin 2006 ni dans ses observations orales formulées par ses représentants lors de la réunion du 28 juin 2006, des informations qui apporteraient des garanties, comme cela était pourtant demandé dans la mise en demeure adoptée par la CNIL le 21 février 2006, sur la régularité de l'inscription de certains requérants (saisines n° 05006569, 05009907 et 05015327), au regard de l'ensemble des dispositions de la loi du 6 janvier 1978 modifiée, au fichier des retraits « CB » mis en œuvre par la Banque de France.

La Commission constate à cet égard que le Crédit Lyonnais n'a jamais communiqué des éléments comptables précis et justifiés sur la nature des incidents de fonctionnement des comptes des requérants liés à l'utilisation d'une carte bancaire, mais a indiqué que les incidents de paiement étaient liés à l'utilisation abusive de formules de chèques ou à l'existence d'échéances impayées relatives à un crédit, et, en aucune manière à l'utilisation d'une carte bancaire. Les informations fournies par le Crédit Lyonnais font même état d'une procédure généralisée visant à inscrire au fichier « CB » de la Banque de France toute personne faisant l'objet d'une procédure de recouvrement ce qui n'est manifestement pas conforme à la réglementation applicable.

Si le Crédit Lyonnais a par ailleurs fait valoir sur ce dernier point que : « dans le cadre de la révision de la procédure de transmission des dossiers litigieux aux

agences de recouvrement, LCL a apporté – dès septembre 2005 – des modifications à la procédure de déclaration d'utilisation abusive de la carte au FCC/CB excluant de ce fait les déclarations de situations similaires à celles objet des réclamations », la CNIL, pour autant, constate qu'elle n'a été informée par le Crédit Lyonnais de l'existence de cette révision de procédure que le 14 juin 2006 alors même que la procédure de mise en demeure avait débuté plusieurs mois auparavant. Elle observe, d'ailleurs, que le Crédit Lyonnais n'a produit aucun document apportant des précisions sur cette nouvelle procédure et constate que celle-ci ne semble pas opérationnelle puisque l'un des requérants (saisine n° 05009907) était toujours inscrit au fichier des retraits « CB » de la Banque de France au jour de la réunion de la formation restreinte du 28 juin 2006 alors même que le Crédit Lyonnais n'avait pas rapporté la preuve à la CNIL de la régularité de cette inscription.

La Commission estime en tout état de cause que le Crédit Lyonnais n'a manifestement pas respecté les conditions d'inscription des requérants au fichier des retraits « CB » visées dans l'arrêté du conseil général de la Banque de France du 16 juillet 1987. Ces faits constituent un manquement aux dispositions de l'arrêté du conseil général de la Banque de France du 16 juillet 1987, notamment son article 2.1 ainsi qu'aux dispositions de la loi du 6 janvier 1978 modifiée le 6 août 2004, notamment son article 6-3° qui dispose qu'un traitement ne peut porter que sur des données à caractère personnel qui sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Ces mêmes faits constituent également un manquement à l'article 6-4° de la loi précitée qui dispose qu'un traitement ne peut porter que sur des données à caractère personnel qui sont exactes.

Ces mêmes faits constituent enfin un manquement à l'article 34 de la loi précitée, s'agissant en particulier de la communication à des tiers (l'ensemble des établissements de crédit ayant communication des coordonnées des personnes physiques inscrites dans le fichier des retraits « CB ») d'informations dont ils n'avaient pas à connaître.

La Commission considère par conséquent que le Crédit Lyonnais n'a pas respecté la mise en demeure adoptée le 21 février 2006 d'apporter toute garantie sur la régularité de l'inscription des requérants, au regard de l'ensemble des dispositions de la loi du 6 janvier 1978 modifiée, au fichier des retraits « CB » mis en œuvre par la Banque de France.

c. Il ressort de l'ensemble de ce qui précède que :

- Le Crédit Lyonnais n'a pas communiqué à la CNIL des informations qu'il avait pourtant bien en sa possession et n'a pas apporté d'éléments de fait permettant de considérer qu'il n'y a pas eu de dissimulation de preuve ou de communication à la CNIL, dans le cadre de l'instruction de la plainte du requérant (saisine n° 04018295) de novembre 2004 à janvier 2006, d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les

demandes ont été formulées par la CNIL notamment dans ses courriers des 15 décembre 2004 et 25 mars 2005.

La Commission relève que ces faits constituent un manquement aux dispositions de la loi du 6 janvier 1978 modifiée, notamment ses articles 21 alinéa 2 et 51.

- le Crédit Lyonnais n'a apporté aucun élément permettant de considérer qu'il a respecté les conditions d'inscription des requérants (saisines n° 05015327, 05006569 et 05009907) au fichier des retraits « CB » visées dans l'arrêté du conseil général de la Banque de France du 16 juillet 1987.

La Commission relève que ces faits constituent un manquement aux dispositions de l'arrêté du conseil général de la Banque de France du 16 juillet 1987, notamment son article 2.1 ainsi qu'aux dispositions de la loi du 6 janvier 1978 modifiée le 6 août 2004, notamment ses articles 6-3°, 6-4° et 34.

La Commission considère en outre qu'en répondant de façon inexacte pendant près d'un an aux demandes de la CNIL alors que les éléments de réponse étaient connus de sa part (saisine n° 04018295) et en ne communiquant à aucun moment à la CNIL les références comptables précises (saisines n° 05006569, 05009907 et 05015327) des incidents de paiement liés spécifiquement à l'utilisation d'une carte bancaire, comme cela lui était pourtant demandé, le Crédit Lyonnais a fait preuve de mauvaise foi.

En conséquence, décide de faire application des dispositions des articles 45 et suivants de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer à l'encontre du Crédit Lyonnais (LCL) sis 18 rue de la République à Lyon (69), compte tenu de la gravité des manquements commis, une sanction pécuniaire équivalente au triple de la somme mise en recouvrement concernant la saisine n° 04018295, soit 30000 euros à laquelle s'ajoutera la somme forfaitaire de 5000 euros pour chacune des saisines n° 05006569, 05015327 et 05009907, soit la somme totale de 45000 euros.

Décide également, compte tenu de la mauvaise foi du Crédit Lyonnais, de la publication de la présente décision, sous la forme d'un extrait tel qu'il figure en annexe à la présente délibération, dans les quotidiens Le Figaro et La Tribune. La publication s'effectuera dans un délai de trente jours à compter du jour où la présente délibération sera devenue définitive et devra être notifiée par le Crédit Lyonnais à la CNIL. Les frais seront supportés par le Crédit Lyonnais.

Le président

Alex Türk

CONSEIL D'ETAT

Statuant au contentieux

N° 212484 212487 212629

Fédération nationale des unions de jeunes avocats et autres

M Mochon, Rapporteur

Mme Maugüé, Commissaire du gouvernement

Lecture du 24 Janvier 2001

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

Vu 1°) sous le n° 212484 la requête, enregistrée le 16 septembre 1999 au secrétariat du contentieux du Conseil d'Etat, présentée par la FEDERATION NATIONALE DES UNIONS DE JEUNES AVOCATS, dont le siège est 4 boulevard du Palais à Paris (75001), représentée par son président ; la FEDERATION NATIONALE DES UNIONS DE JEUNES AVOCATS demande au Conseil d'Etat d'annuler pour excès de pouvoir l'arrêté du garde des sceaux, ministre de la justice du 18 juin 1999 portant création d'un traitement automatisé d'informations à caractère personnel, relatif à la gestion du suivi des affaires pénales par le parquet général des cours d'appel ;

Vu 2°) sous le n° 212487 la requête, enregistrée le 17 septembre 1999 au secrétariat du contentieux du Conseil d'Etat, présentée par l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE, dont le siège est 17/19 rue Pasteur Valléry Radot à Créteil (94011

cedex), représenté par son bâtonnier ; l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE demande au Conseil d'Etat d'annuler pour excès de pouvoir l'arrêté du garde des sceaux, ministre de la justice du 18 juin 1999 portant création d'un traitement automatisé d'informations à caractère personnel, relatif à la gestion du suivi des affaires pénales par le parquet général des cours d'appel ;

Vu le nouveau mémoire, enregistré le 11 décembre 2000, présenté par l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE, qui se désiste de ses conclusions formées sous le n° 212487 ;

Vu 3°) sous le n° 212629, la requête et le mémoire complémentaire, enregistrés les 17 septembre et 15 octobre 1999 au secrétariat du contentieux du Conseil d'Etat, présentés par M Bernard POIRREZ dont le domicile est 82 rue des Carrouges à Noisy-le-Sec (93130) ; M POIRREZ demande : 1) à titre principal l'annulation pour excès de pouvoir de l'arrêté du garde des sceaux, ministre de la justice du 18 juin 1999 portant création d'un traitement automatisé d'informations à caractère personnel, relatif à la gestion du suivi des affaires pénales par le parquet général des cours d'appel ; 2) à titre subsidiaire qu'il plaise au Conseil d'Etat de surseoir à statuer dans l'attente d'une réponse de la Cour de justice des communautés européennes à une question préjudicielle relative à la compatibilité de l'arrêté attaqué avec l'article 6 du traité sur l'Union européenne ;

Vu les autres pièces des dossiers ;

Vu la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

Vu le traité sur l'Union européenne et le traité du 25 mars 1957 instituant la Communauté européenne ;

Vu la loi n° 78-17 du 6 janvier 1978, modifiée par la loi n° 92-1336 du 16 décembre 1992 ;

Vu le code de procédure pénale, notamment ses articles 32 à 38 ;

Vu le décret n° 90-115 du 2 février 1990 ;

Vu le code de justice administrative ;

Après avoir entendu en audience publique :

- ▶ le rapport de M Mochon, Auditeur,
- ▶ les conclusions de Mme Maugüé, Commissaire du gouvernement ;

Considérant que les requêtes de la FEDERATION NATIONALE DES UNIONS DE JEUNES AVOCATS, de l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE et de M POIRREZ, sont dirigées contre un même arrêté ; qu'il y a lieu de les joindre pour qu'elles fassent l'objet d'une même décision ;

Considérant que par un mémoire enregistré au secrétariat du contentieux du Conseil d'Etat le 11 décembre 2000 l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE s'est désisté de sa requête ; que ce désistement est pur et simple ; que rien ne s'oppose à ce qu'il en soit donné acte ;

Considérant que le premier alinéa de l'article 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose qu'il est "interdit de mettre ou de conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales" ou encore, ainsi qu'est venu le spécifier l'article 257 de la loi n° 92-1336 du 16 décembre 1992, "les moeurs des personnes" ; qu'indépendamment de la non-application de cette interdiction dans le cas des groupements mentionnés au deuxième alinéa de l'article 31, en ce qui concerne le registre de leurs membres, le troisième alinéa du même article a prévu que pour des motifs d'intérêt public" il peut aussi être fait exception à l'interdiction sur avis conforme de la Commission nationale de l'informatique et des libertés par décret en Conseil d'Etat ;

Considérant que, sur le fondement du troisième alinéa de l'article 31 de la loi précitée, le décret n° 90-115 du 2 février 1990 a autorisé les juridictions de l'ordre judiciaire et de l'ordre administratif, pour l'exercice de leur mission, à mettre ou conserver en mémoire informatisée les données nominatives nécessaires à l'instruction et au jugement des litiges dont elles sont saisies et à l'exécution des décisions de justice, qui font apparaître, directement ou indirectement, les origines raciales ou les opinions politiques, philosophiques

ou religieuses, ou les appartenances syndicales "des parties au litige" ; que ces dispositions, eu égard à la date d'intervention du décret du 2 février 1990, ne permettent pas de déroger à l'interdiction résultant de l'adjonction apportée au premier alinéa de l'article 31 de la loi du 6 janvier 1978 par celles du 16 décembre 1992, et prohibant la conservation des données nominatives qui concernent les "moeurs" des personnes, sauf consentement de leur part ;

Considérant qu'en cet état du droit le garde des sceaux, ministre de la justice a pris le 18 juin 1999 un arrêté portant création d'un traitement automatisé d'informations à caractère personnel relatif à la gestion du suivi des affaires pénales par le parquet général des cours d'appel dont la légalité est contestée tant par la FEDERATION NATIONALE DES UNIONS DE JEUNES AVOCATS que par M POIRREZ ;

Sur la légalité externe :

Considérant que, par arrêté du 22 mai 1998 publié au Journal officiel du 23 mai 1998 M de Gouttes, directeur des services judiciaires au ministère de la justice avait reçu délégation du ministre, pour signer les arrêtés, actes et décisions ressortissant à ses attributions, au nombre desquels figure l'arrêté attaqué dès lors qu'en vertu d'un précédent arrêté du 1er mars 1988 la direction des affaires judiciaires est en charge de la définition de la politique d'informatisation des juridictions ; que, l'absence, dans les visas de l'arrêté attaqué, de la mention de la délégation de signature est sans incidence sur sa régularité ;

Sur la légalité interne :

Considérant que l'article 1er de l'arrêté attaqué autorise la mise en oeuvre au parquet général des cours d'appel d'un système automatisé de suivi administratif des affaires pénales générales, financières et commerciales ; qu'en vertu du premier tiret de l'article 3 de l'arrêté, les informations saisies dans ce traitement sont, s'agissant des témoins assistés, des personnes mises en examen, des prévenus, des accusés ainsi que des personnes mises en cause dans une enquête préliminaire ou de flagrance lorsqu'il en est rendu compte par le procureur de la République au parquet général, le nom, le nom d'alias le cas d'échéant, les prénoms, la date de naissance, le sexe, la nationalité, la profession, l'adresse ou le lieu de détention, les infractions reprochées et les décisions judiciaires intervenues ; qu'en vertu du deuxième tiret sont saisis, s'agissant des parties civiles, civilement responsables, plaignants, victimes, témoins, représentants légaux, le nom ou la raison sociale pour les personnes morales, les prénoms, le sexe, l'adresse ou le domicile élu et la qualité ; qu'en vertu du troisième tiret sont saisis, s'agissant des avoués, avocats, huissiers, notaires, experts judiciaires,

mandataires de justice, magistrats consulaires, le nom, le prénom et le numéro de téléphone professionnel ; qu'en vertu du quatrième tiret sont saisis, s'agissant des magistrats en charge du dossier, la fonction, le nom et le prénom ;

En ce qui concerne les moyens tirés de la violation du décret du 2 février 1990 :

Quant aux deuxième, troisième et quatrième tirets de l'article 3 de l'arrêté attaqué :

Considérant que les dispositions précitées du décret du 2 février 1990, sur le fondement desquelles est autorisé le traitement automatisé des informations en cause, régissent le seul traitement des informations qui, faisant apparaître directement ou indirectement les origines raciales ou les opinions politique, philosophiques ou religieuses ou les appartenances syndicales des parties au litige, relèvent de l'article 31 de la loi du 6 janvier 1978 dans sa rédaction en vigueur à la date d'intervention du décret précité ; que le décret n'a ni pour objet ni pour effet de faire obstacle à la saisie et à la conservation dans les traitements mis en oeuvre par les juridictions d'informations autres que celles ayant motivé son intervention, sous la réserve qu'ils ne soit pas dérogé à l'interdiction issue de l'article 257 de la loi du 16 décembre 1992 de conserver des données nominatives concernant les "moeurs" des personnes en cause ;

Quant au premier tiret de l'article 3 de l'arrêté attaqué :

Considérant que les informations dont l'arrêté attaqué autorise le traitement et qui concernent les personnes mises en examen, les prévenus, les accusés ainsi que les témoins assistés visent des personnes qui ont la qualité de "parties au litige" au sens des dispositions du décret du 2 février 1990 ; qu'en outre, les informations dont le traitement est autorisé sont nécessaires à l'instruction du litige et le cas échéant à son jugement ; qu'ainsi les requérants ne sont pas fondés à soutenir que l'article 3 de l'arrêté attaqué, en tant qu'il se réfère aux catégories de personnes ci-dessus énumérées, serait contraire au décret ;

Considérant, en revanche, que les personnes mises en cause dans une enquête préliminaire ou de flagrance, alors même qu'il en est rendu compte par le procureur de la République au parquet général en application de l'article 35 du code de procédure pénale, ne sont pas nécessairement appelées à être des parties à un litige devant une juridiction d'instruction ou de jugement ; qu'ainsi, en tant qu'il autorise la mise en mémoire et la conservation d'informations relatives aux infractions reprochées aux personnes mises en cause dans une enquête préliminaire ou de flagrance, l'arrêté attaqué méconnaît le décret du 2 février 1990 ; qu'il doit dans cette mesure, être annulé ;

En ce qui concerne la violation alléguée de l'article 6 du traité sur l'Union européenne :

Considérant qu'en vertu du paragraphe 2 de l'article 6 du traité sur l'Union européenne, l'Union respecte les droits fondamentaux "tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres, en tant que principes généraux du droit communautaire" ;

Considérant que M POIRREZ soutient que l'arrêté attaqué méconnaîtrait les stipulations précitées de l'article 6 du fait qu'il serait contraire au droit au respect de la vie privée garanti par le paragraphe 1 de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; qu'il est demandé au Conseil d'Etat de surseoir à statuer jusqu'à ce que la Cour de justice des Communautés européennes, saisie à titre préjudiciel sur le fondement de l'article 177 du traité de Rome devenu l'article 234 du traité CE, se soit prononcée sur la portée à donner à l'article 8 de la convention ;

Considérant qu'il résulte de l'article 46 du traité sur l'Union européenne que les dispositions des traités communautaires qui sont relatives à la compétence de la Cour de justice des Communautés européennes et à l'exercice de celle-ci ne sont applicables, s'agissant de l'article 6, paragraphe 2, du traité sur l'Union "qu'en ce qui concerne l'action des institutions" ; qu'il suit de là que le renvoi préjudiciel sollicité est dépourvu de pertinence ;

Considérant, en outre, qu'en admettant même que la protection des données à caractère personnel entre dans le champ des prévisions du paragraphe 1 de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, les dispositions réglementaires dont M POIRREZ conteste la légalité trouvent un fondement dans les stipulations du paragraphe 2 de l'article 8 de la convention précitée ;

Considérant qu'il résulte de tout ce qui précède que, par les moyens qu'ils invoquent, les requérants ne sont fondés à demander l'annulation de l'arrêté attaqué que dans la mesure où, par son article 3, il autorise la mise en mémoire et la conservation d'informations relatives aux infractions reprochées aux personnes mises en cause dans une enquête préliminaire ou de flagrance ;

D E C I D E :

Article 1er : Il est donné acte du désistement de la requête de l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE.

Article 2 : L'article 3 de l'arrêté du 18 juin 1999 du garde des sceaux ministre de la justice est annulé en tant qu'il autorise la mise en mémoire et la conservation d'informations relatives aux infractions reprochées aux personnes mises en cause dans une enquête préliminaire ou de flagrance.

Article 3 : Le surplus des conclusions de la FEDERATION NATIONALE DES UNIONS DE JEUNES AVOCATS et de M POIRREZ est rejeté.

Article 4 : La présente décision sera notifiée à la FEDERATION NATIONALE DES UNIONS DE JEUNES AVOCATS, à l'ORDRE DES AVOCATS DU BARREAU DU VAL-DE-MARNE, à M Bernard POIRREZ et au garde des sceaux, ministre de la justice.

Commission nationale de l'informatique et des libertés

Délibération n°2006-281 du 14 décembre 2006
sanctionnant
la société Tyco Healthcare France

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK ;

Etant aussi présents M. Guy ROSIER, vice-président délégué, M. François GIQUEL, vice-président, M. Hubert BOUCHET, membre, Mlle Anne DEBET, membre et M. Bernard PEYRAT, membre ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n°2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2006-144 adoptée par la CNIL le 10 mai 2006 ;

Vu la décision de mission de contrôle n° 2006-074C ;

Vu le rapport de M. Emmanuel de GIVRY, commissaire, notifié à la société Tyco Healthcare France le 27 octobre 2006 et les observations en réponse reçues le 24 novembre 2006.

Après avoir entendu, lors de la réunion du 14 décembre 2006, M. Emmanuel de GIVRY, commissaire, en son rapport et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations.

Après avoir entendu, lors de la réunion du 14 décembre 2006, les observations orales de Maître LORELEI, avocat, représentant la société Tyco Healthcare France, celle-ci ayant pris la parole en dernier.

Constata les faits suivants :

1. La société Tyco Healthcare France a déclaré à la CNIL le 22 septembre 2004 un traitement de données ayant pour finalité la « gestion des carrières à l'international ».

Par courrier en date du 21 février 2005, la CNIL lui a demandé de lui faire parvenir certains éléments d'information indispensables à l'instruction de ce dossier. La société Tyco Healthcare France n'a apporté aucune suite satisfaisante aux demandes de la Commission réitérées dans ses courriers des 19 septembre 2005 et 21 mars 2006.

En effet, la réponse adressée par la société Tyco Healthcare France SAS le 4 avril 2006 n'a pas permis d'apporter les réponses à l'ensemble des questions formulées par les services de la CNIL dans le cadre de l'instruction du dossier de déclaration (le descriptif précis des finalités exactes recherchées, les cas précis dans lesquels des données à caractère personnel sont envoyées en Grande-Bretagne et aux Etats-Unis, les lieux exacts d'implantation des serveurs et des systèmes, les fonctionnalités précises de l'application, les destinataires exacts des données, les mesures de sécurité assurant la confidentialité des données et la durée de conservation des données).

2. Au regard des faits précités, la Commission a, par délibération adoptée le 10 mai 2006, mis en demeure la société Tyco, sous dix jours, de répondre aux questions posées par la CNIL dans ses courriers (courriers des 21 février, 19 septembre 2005, 21 mars 2006) ou de lui indiquer que le traitement précité avait été abandonné.

3. En réponse à la mise en demeure, la société Tyco Healthcare France a indiqué, par courrier du 1er juin 2006, que : « Le groupe Tyco au niveau international devait scinder les 4 secteurs d'activités qui le constituent actuellement en entités indépendantes. Cette scission doit intervenir d'ici la fin de l'année calendaire. Par conséquent les procédures et les demandes d'information qui avaient été mises en place sont dans les circonstances actuelles suspendues ».

4. La CNIL ne s'estimant pas suffisamment informée par cette réponse sur le sort exact ayant été finalement réservé au traitement objet de la mise en demeure a fait procéder à une mission de contrôle sur place le 12 juillet 2006 dans les locaux de la société Tyco Healthcare France.

A cette occasion, les services de la CNIL ont constaté que le traitement objet de la mise en demeure, contrairement à ce qui avait été affirmé, était bien utilisé par la société Tyco Healthcare France.

Au regard des documents communiqués (« International Database Project Update, Data Auditing and Next Steps, June 2006 » et « Guide de l'administrateur, Administration et traitement des données pour la base de données internationales »), le traitement précité apparaît comme un outil de gestion essentiel, au plan mondial, de la politique salariale du groupe Tyco dont les finalités dépassent largement la finalité de « reporting » visée dans la déclaration du 22 septembre 2004. Lors de la mission de contrôle sur place, il a également été constaté que de strictes et récentes procédures étaient mises en œuvre pour que la société Tyco Healthcare France alimente de façon régulière la base de données avec les informations concernant les salariés français.

5. Il ressort de ce qui précède que les faits constatés sur place le 12 juillet 2006 étaient en contradiction avec la réponse adressée par la société Tyco Healthcare France le 1er juin 2006 puisque celle-ci n'a ni « suspendu » la mise en œuvre du traitement objet de la mise en demeure ni répondu à l'ensemble des questions posées concernant les modalités exactes de fonctionnement du traitement précité.

En effet, s'agissant tout d'abord du descriptif précis des finalités recherchées et des fonctionnalités de l'application, dans son courrier du 4 avril 2006 la société Tyco Healthcare France indique que « la finalité de

cette base de données est purement celle d'un « reporting » vis à vis de notre hiérarchie européenne en ressources humaines ».

Un document interne datant de juin 2006 communiqué aux services de la CNIL lors de la mission de contrôle du 12 juillet 2006 indique pourtant (« International Database Project Update, Data Auditing and Next Steps, June 2006 »), concernant le traitement précité, que celui-ci sert à la gestion des stock-options, la formation professionnelle, le niveau des rémunérations, la communication professionnelle, etc. Lors de la réunion du 14 décembre 2006, l'avocat représentant la société Tyco Healthcare France a également indiqué oralement que le traitement objet de la mise en œuvre avait également pour finalité de gérer la « mobilité interne ».

Dès lors, la Commission ne s'estime toujours pas informée sur le descriptif précis des finalités recherchées par le traitement déclaré le 22 septembre 2004 par la société Tyco Healthcare France comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

S'agissant ensuite des cas précis dans lesquels des données à caractère personnel sont envoyées dans les locaux du groupe Tyco en Grande-Bretagne et aux Etats-Unis, le courrier du 4 avril 2006 se limite à indiquer que « ces données peuvent être transmises du Royaume-Uni aux Etats-Unis si notre hiérarchie juge opportun de le faire ».

Si le contrôle du 12 juillet 2006 a permis d'établir une communication d'informations concernant le traitement objet de la mise en demeure entre la société Tyco Healthcare France et les locaux du groupe Tyco en Angleterre et aux Etats-Unis, il n'a pas été possible d'obtenir des informations précises sur les motifs liés à cet envoi d'informations.

Dès lors, la Commission ne s'estime toujours pas correctement informée des cas précis où des données à caractère personnel sont envoyées dans les locaux du groupe Tyco en Grande-Bretagne et aux Etats-Unis comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

S'agissant encore des lieux exacts d'implantation des serveurs et des systèmes, seul un schéma technique a été communiqué aux services de la Commission (« Schéma de fonctionnement informatique Tyco Healthcare France ») mais les adresses exactes des centres informatiques n'ont pas été communiquées à ce jour.

S'agissant des questions posées concernant les destinataires exacts des données et la durée de conservation des données, la Commission ne dispose à ce jour d'aucune réponse précise.

S'agissant enfin des mesures de sécurité assurant la confidentialité des données, si la mission de contrôle du 12 juillet 2006 a permis d'établir que l'accès aux ordinateurs de la société Tyco Healthcare France est sécurisé par mot de passe, la Commission ne dispose à ce jour d'aucune information technique précise sur les conditions de sécurité liées à la conservation des données en Angleterre et aux Etats-Unis.

Dès lors, la Commission ne s'estime toujours pas correctement informée sur les lieux exacts d'implantation des serveurs et des systèmes, les destinataires exacts des données, la durée de conservation des données et les mesures de sécurité assurant la confidentialité des données comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

6. Dans ses observations en réponse du 24 novembre 2006 et lors de la réunion du 14 décembre 2006, la société Tyco Healthcare France soutient que la proposition de sanction proposée par le rapporteur serait mal fondée sur le plan juridique dans la mesure où celle-ci ne s'appuierait sur aucune mise en demeure préalable mais uniquement sur la réalisation de la mission de contrôle du 12 juillet 2006.

Sur ce point, la Commission observe qu'une procédure de sanction peut être engagée lorsque le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée (article 45 de la loi du 6 janvier 1978 modifiée le 6 août 2004). La présente procédure de sanction s'appuie ainsi sur la mise en demeure prononcée par la CNIL le 10 mai 2006 et sur la réponse adressée par la société Tyco le 1er juin 2006.

Il convient par ailleurs de rappeler que dans le cadre de l'analyse de la réponse adressée par la société Tyco le 1er juin 2006, la CNIL était en droit de procéder à une mission de vérification sur place afin, de vérifier la réalité des informations qui lui avaient été communiquées. La Commission estime à cet égard que les informations transmises par la société Tyco Healthcare France dans son courrier du 1er juin 2006 ne permettaient pas de connaître le sort exact ayant été réservé au traitement objet de la mise en demeure du 10 mai 2006.

Au surplus, la société Tyco Healthcare France relève dans ses observations du 24 novembre 2006 que la décision de mission de contrôle n° 2006-074C ne visait pas formellement la mise en demeure du 10 mai 2006. Sur ce point, la Commission estime que l'existence d'une procédure de mise en demeure n'a, à cet égard, aucune incidence sur le formalisme à respecter pour la réalisation d'une telle mission de contrôle.

La Commission considère par conséquent que la procédure de sanction est pleinement régulière.

7. La société Tyco a par ailleurs fait valoir dans ses observations du 24 novembre 2006 et lors de la réunion du 14 décembre 2006 que les informations communiquées lors de la mission de contrôle ne concerneraient pas le même traitement que celui visé dans la mise en demeure du 10 mai 2006.

La Commission observe que les vérifications opérées sur place le 12 juillet 2006 par les services de la CNIL ont permis de constater que le traitement déclaré par la société Tyco Healthcare France le 22 septembre 2004 (« gestion des carrières à l'international »), comportait, comme indiqué précédemment, d'autres fonctionnalités relatives à la gestion des ressources humaines telles que par exemple la gestion des stock-options, la formation professionnelle, le niveau des rémunérations, la communication professionnelle ainsi que la mobilité interne.

Ces fonctionnalités, qui peuvent être rattachées à une finalité de gestion des carrières à l'international, n'étaient pas décrites dans la déclaration adressée par la société Tyco Healthcare France le 22 septembre 2004.

La Commission observe par ailleurs que les captures d'écran réalisées par les services de la CNIL lors du contrôle du 12 juillet 2006 sont concordantes s'agissant des catégories de données collectées et utilisées avec les « champs » informatiques figurant dans la déclaration adressée par la société Tyco Healthcare France le 22 septembre 2004 (données démographiques concernant les salariés, données sur la situation administrative des salariés, données concernant la localisation géographique des salariés, données sur la rémunération des salariés, etc.).

Dès lors, la Commission considère que les vérifications opérées par la CNIL le 12 juillet 2006 concernaient bien le traitement visé dans la mise en demeure du 10 mai 2006.

8. Il ressort de l'ensemble de ce qui précède que la société Tyco Healthcare France ne s'est pas conformée à la mise en demeure de la CNIL du 10 mai 2006 puisqu'elle n'a pas communiqué les éléments demandés par la CNIL concernant le traitement déclaré le 22 septembre 2004 (le descriptif précis des finalités exactes recherchées, le cas précis dans lesquels des données à caractère personnel sont envoyées en Grande-Bretagne et aux Etats-Unis, les lieux exacts d'implantation des serveurs et des systèmes, les fonctionnalités précises de l'application, les destinataires exacts des données, les mesures de sécurité assurant la confidentialité des données et la durée de conservation des données) et qu'elle n'a pas cessé la mise en œuvre de celui-ci.

La Commission observe à cet égard que la société Tyco Healthcare France n'a manifestement pas pris la mesure de la gravité des manquements qui lui sont reprochés concernant son manque de coopération et de transparence.

En conséquence, la Commission décide de faire application des dispositions des articles 45 et suivants de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer à l'encontre de la société Tyco Healthcare France sise 2 rue Denis Diderot, La clef de Saint Pierre à Elancourt (78), compte tenu de la gravité des manquements commis, une sanction pécuniaire de 30.000 euros.

Par ailleurs, la Commission enjoint la société Tyco Healthcare France de répondre, sous dix jour à compter de la notification de la présente délibération, à l'ensemble des demandes formulées par la CNIL dans sa mise en demeure du 10 mai 2006.

La présente décision sera rendue publique.

Le président, Alex Türk

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

**Délibération n° 2007-374 du 11 décembre 2007 sanctionnant
la société SERVICE INNOVATION GROUP FRANCE**

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK ;

Etant aussi présents, M. François GIQUEL, vice-président, Mlle Anne DEBET, membre, M. Hubert BOUCHET, membre ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2007-228 mettant en demeure la société SIG, adoptée par la CNIL le 10 juillet 2007 ;

Vu la décision n° 2006-112 C en date du 5 décembre 2006 du président de la Commission nationale de l'informatique et des libertés de procéder à une mission de contrôle auprès de la société SERVICE INNOVATION GROUP France ;

Vu le rapport de M. Jean MASSOT, commissaire, remis en mains propres le 9 novembre 2007 et les observations en réponse reçues, par télécopie le 7 décembre 2007 et par courrier le 10 décembre 2007.

Après avoir entendu, lors de la réunion du 11 décembre 2007, M. Jean MASSOT, commissaire, en son rapport et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations.

Après avoir entendu, lors de l'audience du 11 décembre 2007, les observations orales de Maître VILLEDIEU avocat, et Mme Sophie BAYLE, directeur général délégué, ceux-ci ayant pris la parole en dernier.

Constate les faits suivants :

1. En application de la décision n° 2006-112C, une délégation de la Commission nationale de l'informatique et des libertés (ci-après « CNIL ») a procédé à une vérification sur place, le 6 décembre 2006, auprès de la société SERVICE INNOVATION GROUP France (ci-après « SIG »), sise 150 rue Gallieni à Boulogne-Billancourt (92100). La délégation de la CNIL s'est attachée à examiner plus particulièrement les traitements du personnel mis en œuvre par la société SIG.

Lors de la mission de contrôle, il a été constaté que les candidats à un emploi pouvaient remplir un *curriculum vitae* en ligne sur le site www.serviceinnovation.fr, au moyen d'un formulaire de collecte de données.

Il a été constaté que ce formulaire ne comportait pas l'information prévue par l'article 32 de la loi du 6 janvier 1978 qui dispose que : « *la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ; de la finalité poursuivie par le traitement auquel les données sont destinées ; du caractère obligatoire ou facultatif des réponses ; des conséquences éventuelles, à son égard, d'un défaut de réponse ; des destinataires ou catégories de destinataires des données ; des droits qu'elle tient*

des dispositions de la section 2 du présent chapitre ; le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ».

La délégation de la CNIL a par ailleurs relevé que les *curriculum vitae* reçus étaient intégrés à la base de données de production dénommé « SEP-SI », avec un statut associé : « 0 : création », « 1 : qualifié », « 2 : Vu + Qualifié ». Seuls les *curriculum vitae* de statuts 1 et 2 étaient inclus dans les recherches informatisées de candidats.

La gestion des salariés, mis à disposition de la clientèle, était également centralisée sur le plan informatique dans l'application « SEP-SI ».

La CNIL a pu constater que certains codes informatiques étaient parfois associés aux fiches de candidats à un emploi et d'anciens salariés, notamment :

- statut « inactif » pour les personnes qui ne sont plus candidates à un emploi, soit de leur fait, soit suite à une décision de la société de ne plus les employer (39000 inactifs sur 60000 fiches, soit 65% des fiches) ;
- code 99 « PNG » pour les personnes ayant déjà été employées et qui n'ont pas donné satisfaction.

S'agissant de l'articulation entre le code « PNG » et le statut « inactif », les représentants de la société SIG, interrogés par la CNIL, n'ont pas apporté de précision particulière.

Le statut « PNG » était enregistré à la suite de l'évaluation de la mission par le chef de secteur. Ce code signifie, d'après la société SIG, « Personne Non Garantie ». Cependant, aucune liste informatique de motifs, justifiant l'inscription du statut « PNG », n'était associée à ce code.

Une copie de la note « *PNG – nouvelle procédure* » du 13 septembre 2001 a été remise à la délégation de la CNIL. Cette note précisait notamment que l'attribution du code 99 « PNG » s'accompagne de la saisie obligatoire d'un texte d'explication. Il a également été indiqué que la mise en code « PNG », et son éventuelle suppression ultérieure, étaient des informations accessibles dans la rubrique « historique » d'une personne.

Cette note ne détaillait pas les cas dans lesquels une personne pouvait se voir attribuer un code « PNG » et n'alertait pas les utilisateurs de la base sur la nature des données pouvant être portées dans les zones de commentaire libre, associées à ce code.

Une copie de la totalité des enregistrements PNG et de leurs commentaires associés a été transmise à la Commission. 4735 personnes ont fait ainsi l'objet d'un codage « PNG ».

La consultation de ces 4735 enregistrements a permis de constater le défaut de pertinence et la nature très subjective de certains commentaires associés.

Ainsi par exemple, les commentaires suivants ont pu être identifiés :

- commentaires subjectifs sur le comportement des personnes (« pas crédible », « 2 tension », « cas social », « catastrophe », « menteuse et pas fiable », « nul », « pas top », « problèmes d'hygiène (odeurs) !!!!! », « trop chiant », etc.) ;
- commentaires faisant référence à des vols commis par les employés (« vol en magasin », « a été soupçonné de vol en FA 2003 », « serait une voleuse », etc.) ;
- commentaires relatifs à l'état de santé des employés (« a disparu suite à une dépression : hospitalisé », « dépressive », « enceinte », « personne sans dents et qui boit », « problèmes alcoolisme », « souffre d'un cancer ne pourra plus travailler », etc.) ;
- commentaires faisant état des relations personnelles ou familiales négatives des employés (« copine de M. - pas fiable », « n'habite plus avec son mari », « femme de G. », etc.) ;

- commentaires relatifs à une procédure prud'homale en cours (« lui confier le plus de travail possible - prud'hommes en cours », « a amené la SEP aux prud'hommes », etc.) ;
- commentaires mentionnant la nouvelle situation professionnelle de l'intéressé (« à la retraite », « a trouvé du travail (rentre dans l'Armée) », « est au chômage mais préfère ne pas travailler », etc.).

De plus, des imprécisions ou des incohérences ont été relevées entre la mise sous code « PNG » et le commentaire associé : « *ne surtout plus faire travailler* », « *PNG mis sans raison connue* », « *ne plus reprendre* », « *PNG mais par qui ?* », « *pourquoi en PNG (aucune raison fait parfaitement son travail)* », etc.

S'il est admis que des traitements de données à caractère personnel peuvent comporter des zones commentaires destinées à enregistrer des informations de gestion, telles des résumés d'entretien ou des indicateurs sur le suivi d'un dossier, ces mentions doivent, comme toute donnée à caractère personnel enregistrée dans un traitement et appelée à y être conservée, être pertinentes, adéquates et non excessives au regard de la finalité du traitement.

La Commission a relevé que les faits précités sont ainsi de nature à constituer un manquement aux obligations découlant du 3° de l'article 6 de la loi du 6 janvier 1978 modifiée qui dispose qu'un traitement ne peut porter que sur des données à caractère personnel (...) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs. Le non-respect de cette obligation est susceptible d'entraîner l'application de l'article 226-18 du code pénal.

La prise en compte d'informations relatives à l'âge, la situation familiale ou le nombre d'enfants à charge dans le cadre de l'attribution d'une mission est susceptible de ne pas être conforme à l'article précité, ni à l'article L.122-45 du code du travail selon lequel aucune personne ne peut être écartée d'une procédure de recrutement notamment en raison de son âge ou de sa situation de famille.

L'article L.121-6 du code du travail dispose également que « *Les informations demandées, sous quelque forme que ce soit, au candidat à un emploi ou à un salarié ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles. Ces informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles* ».

Par ailleurs, plusieurs commentaires relatifs à des anciens salariés ne sont manifestement pas conformes aux dispositions du 1° de l'article 6 de la loi du 6 janvier 1978 modifiée qui dispose qu'un traitement ne peut porter que sur des données à caractère personnel (...) collectées et traitées de manière loyale et licite.

L'analyse des fichiers contrôlés permet en outre de considérer que l'article 8 de la loi du 6 janvier 1978 modifiée n'a pas été respecté. Aux termes de ces dispositions, il est interdit de collecter ou de traiter des données à caractère personnel relatives à la santé, sauf, dans la mesure où la finalité du traitement l'exige, si notamment la personne concernée a donné son consentement exprès, c'est-à-dire écrit.

Il en est de même concernant l'article 9 de la loi du 6 janvier 1978 modifiée qui dispose que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre, notamment, que par les juridictions et les auxiliaires de justice.

Le non-respect des deux articles susvisés est susceptible d'entraîner l'application de l'article 226-19 du code pénal.

En outre, aux termes de l'article L.121-8 du même code pénal : « *Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.* »

De plus, aux termes de l'article 32 de la loi du 6 janvier 1978 modifiée, la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant, notamment de la finalité poursuivie par le traitement auquel les données sont destinées.

Enfin, il convient de rappeler que conformément aux dispositions de l'article 39 de la loi du 6 janvier 1978 modifiée, toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir la communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci.

Par conséquent, toute personne doit être informée, par tout moyen, des finalités du traitement où sont enregistrées des données personnelles la concernant, à savoir la gestion et l'évaluation des candidats à un emploi ; de même, toute personne faisant l'objet d'une codification « PNG » et exerçant son droit d'accès auprès de la société SIG doit être informée de l'existence de cette codification ainsi que des raisons précises pour lesquelles une telle décision a été prise à son égard. Or, il apparaît qu'aucune procédure n'a manifestement été mise en œuvre au sein de la société SIG afin qu'une telle information soit communiquée aux intéressés.

Conformément au 5° de l'article 6 de la loi du 6 janvier 1978 modifiée, les données personnelles ne peuvent être conservées au-delà de la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Il apparaît qu'aucune durée de conservation n'a été fixée dans le cadre de la base de données de production, qui comporte l'ensemble des informations concernant les salariés et candidats à un emploi, dont environ 39 000 enregistrements de fiches inactives sur un total de 60 000 fiches ainsi que l'ensemble des *curriculum vitae* finalement non retenus et des personnes mises sous code PNG depuis plusieurs années.

Enfin, il ressort des informations communiquées par les représentants de la société SIG que le traitement de recrutement et de gestion du personnel, ainsi que d'autres traitements tels que les dispositifs de contrôle des horaires, la base de gestion de la clientèle et les traitements relatifs au contrôle de l'utilisation d'internet définis dans le cadre d'une charte informatique, ont été mis en œuvre sans avoir été préalablement déclarés à la CNIL.

Seules deux déclarations simplifiées, à l'ancien nom de la société (SEP Sales et Promotion), ont été réalisées en 1981 pour la paie et la gestion des personnels, et en 2001 pour la mise en place d'un autocommutateur téléphonique.

En conséquence, par délibération n° 2007-228 du 10 juillet 2007, la Commission a mis en demeure la société SIG, sise 150 rue Gallieni à Boulogne-Billancourt (92100), sous un délai d'un mois à compter de la notification de la décision (le 28 août 2007) de :

- procéder à l'accomplissement des formalités préalables auprès de la CNIL pour tout traitement automatisé de données à caractère personnel mis en œuvre ;
- procéder à la suppression de l'ensemble des commentaires associés au code « PNG » susceptibles de ne pas être conformes aux articles 6-1°, 6-3°, 8 et 9 de la loi du 6 janvier 1978 modifiée ;
- apporter des explications sur la finalité exacte du statut « inactif » au regard de l'utilisation éventuelle du code « PNG » ;

- définir, dans le cadre d'une procédure interne, une liste de critères objectifs susceptibles d'entraîner l'utilisation du code « PNG » ou du statut « inactif » et procéder à une revue complète des 4735 anciens salariés faisant actuellement l'objet de la codification « PNG » ;
- apporter toute justification (sensibilisation du personnel, contrôles réguliers du contenu des fichiers, etc.) permettant à la CNIL de considérer que les manquements qui ont été constatés ne se reproduiront pas à l'avenir ;
- justifier les raisons pour lesquelles les informations relatives à l'âge, la situation familiale ou le nombre d'enfants à charge sont utilisées dans le cadre de l'attribution des missions temporaires, ou, à défaut, de les supprimer ;
- apporter toute justification attestant que des mentions d'information conformes aux dispositions de l'article 32 de la loi précitée seront bien apposées sur tout support approprié ainsi que sur l'ensemble des formulaires de collecte de données utilisés par la société SIG ;
- communiquer à la CNIL l'intégralité des mesures prises au sein de la société SIG visant à respecter les dispositions des articles 38 (droit d'opposition), 39 (droit d'accès, s'agissant, notamment, du droit d'accès à l'existence de la codification « PNG » et aux commentaires associés) et 40 (droit de rectification) de la loi du 6 janvier 1978 modifiée ;
- définir, pour l'ensemble des traitements mis en œuvre par la société SIG, une durée de conservation adéquate et proportionnée à la finalité du traitement, s'agissant, notamment, des fiches informatiques utilisant la codification « PNG » et des fiches informatiques en statut « inactif ».

2. En réponse à la mise en demeure, la société SIG a adressé à la CNIL un courrier, en date du 10 septembre 2007, dans lequel elle soutient s'être conformée aux dispositions de la loi du 6 janvier 1978 modifiée. Elle a également précisé qu'elle a fusionné avec la société B&W Marketing et a indiqué que « *l'outil informatique décrié* » a été abandonné au profit du système automatisé de gestion du personnel, initialement mis en œuvre par la société B&W Marketing.

3. Le 24 octobre 2007, la CNIL a décidé de procéder à une seconde mission de contrôle auprès de la société SIG, sise désormais 34 avenue de l'Europe à Vélizy-Villacoublay (78941), afin de vérifier si elle s'était réellement mise en conformité avec les termes de la mise en demeure, en particulier si le précédent outil était effectivement abandonné et si la nouvelle base de données était conforme aux exigences de la loi du 6 janvier 1978 modifiée.

Lorsque les agents de la CNIL ont opéré le contrôle pour vérifier la conformité d'un traitement mis en œuvre par la société SIG aux exigences de la loi du 6 janvier 1978 modifiée, ils ne se sont pas limités à la vérification d'un seul fichier mais se sont intéressés à toutes les applications informatiques poursuivant la ou les finalités du traitement concerné.

La délégation de la Commission a constaté que l'application « SEP-SI » n'a pas vocation à perdurer au sein de la société SIG mais qu'elle devait cependant être maintenue jusqu'à la fin du mois d'octobre 2007, s'agissant de certaines opérations relatives à la paie et à la comptabilité d'un client. Cette pratique est contraire à ce qui était indiqué dans le courrier de la société SIG en date du 10 septembre 2007.

Il a par ailleurs été relevé que la société SIG utilisait principalement le système d'information « KHEOPS », qui était l'outil exploité par la société B&W Marketing. Cette application contenait les fiches du personnel actuel de la société SIG, dont celles des personnes ayant travaillé pour la société B&W Marketing, mais ne comprenait plus les données personnelles relatives aux candidatures.

En outre, l'exploitation des extractions opérées lors de ce contrôle, a démontré que des commentaires non pertinents et de nature subjective, associés aux fiches du personnel, figuraient toujours dans les systèmes d'information « SEP-SI » et « KHEOPS », mis en œuvre par la société SIG. Ainsi, à titre d'exemple, les commentaires suivants ont pu être relevés :

- sur le comportement des personnes : « *ne pas lui proposer de ponctuel très conne* », « *pas sympa* », « *cerveau de dinosaure* », « *a l'air très chiante* », « *grosse menteuse* », « *ne pas appeler avant 16h car mari très con* », « *pb obsédé sexuel* », « *c'est dame qui pue* », etc. ;

- sur les vols commis par les personnes : « *en cours de licenciement vol* », « *ne plus jamais faire travailler : a volé dans 2 magasins* », « *interdit tout magasin accuse vol* », etc. ;
- sur l'état de santé des personnes : « *ne jamais faire travailler : alcoolique* », « *malade d'un cancer mais veut reprendre le W en sept2007* », « *à éviter : dépressive* », « *travaille avec bonnet cause de névralgies* », etc. ;
- sur les relations personnelles ou familiales négatives des personnes : « *attention femme A. S.* », « *copain de la sœur a O. M.* », etc. ;
- sur les procédures prud'homales en cours : « *ne plus faire travailler, gros PB Prud'homme* », « *nous a emmené au prud'homme* », etc.
- autres commentaires de nature subjective : « *trop vieille NESTLE* », « *Bien mais un peu âgée* », « *par sur l'alcool (religion oblige)* », « *à ne jamais faire travailler* », « *A éviter fortement* », etc.

4. Sur la base des constatations opérées par la CNIL lors de cette seconde mission de contrôle, une proposition de sanction a été notifiée à la société SIG, le 9 novembre 2007. Il ressortait des conclusions du rapporteur que les manquements identifiés par la CNIL demeuraient à l'issue de la seconde mission de contrôle sur place.

Le 7 décembre 2007, la société SIG a adressé à la CNIL ses observations en réponse.

a) S'agissant de l'obligation de déclaration du traitement mis en œuvre par la société SIG, la Commission observe qu'elle n'a pas effectué de modification de l'engagement de conformité à la norme simplifiée n° 7 relative à la paie et la gestion des personnels, enregistré auprès de la CNIL en 1981, ni de déclaration normale s'agissant traitement dénommé « KHEOPS ».

Dans ses observations écrites en date du 7 décembre 2007, la société SIG a précisé que l'application « KHEOPS » est en cours d'adaptation et que la déclaration de ce traitement n'est qu'au stade de projet dans la mesure où les annexes techniques ne peuvent être encore remplies.

Dans ces conditions, la Commission estime que la société SIG ne s'est pas conformée, sur ce point, à la mise en demeure qui lui a été adressée car le traitement KHEOPS a été mis en œuvre depuis juillet 2007. Or, le chapitre IV de la loi du 6 janvier 1978 prévoit précisément les formalités à accomplir auprès de la CNIL préalablement à la mise en œuvre des traitements.

b) La délégation de la CNIL a constaté, lors de la seconde mission de contrôle, que la société SIG n'avait pas pris les mesures nécessaires visant à mettre fin au manquement à l'obligation de pertinence, d'adéquation et du caractère non-excessif des données au regard de la finalité du traitement, objet de la mise en demeure. En effet, les commentaires cités plus haut ne sont pas conformes à la loi du 6 janvier 1978 modifiée, notamment à ses articles 6 et 8, figuraient toujours dans les systèmes d'information « SEP-SI » et « KHEOPS ».

Dans ses observations écrites du 7 décembre 2007 et orales, prononcées lors de l'audience du 11 décembre 2007, la société SIG a affirmé à la formation restreinte de la CNIL avoir supprimé l'intégralité des commentaires litigieux.

La Commission observe que la société SIG produit, à l'appui de ses observations écrites du 7 décembre 2007, une facture établie par la société PHIDIAS, le 22 novembre 2007, qui précise la « *suppression ou la transformation de zones inutilisées* » dans l'application KHEOPS. Dans ses observations orales à l'audience du 11 décembre 2007, l'avocat de la société SIG a indiqué que ces zones ne permettraient plus que l'enregistrement du courriel de la personne concernée. La Commission rappelle que lors du contrôle du 24 octobre 2007, la représentante de la société SIG avait déjà affirmé que les

zones commentaires ne servaient qu'à l'enregistrement du courriel. La délégation de la CNIL avait pourtant constaté que ces zones commentaires comportaient les appréciations précitées.

La délégation de la CNIL a par ailleurs relevé, lors de la seconde mission de contrôle, que les fiches du personnel pouvaient être marquées des statuts « *incident bloquant* » ou « *incident majeur* » lorsqu'un employé connaît un problème avec un client ou dans un magasin. L'événement bloque toute relation professionnelle entre les personnes concernées. La société SIG exclut donc le salarié d'un droit ou d'un contrat, au sens de la loi du 6 janvier 1978 modifiée.

A la suite de plusieurs « *incidents* », la fiche d'un intervenant peut être marquée du statut « *inactif* » si la société SIG décide de ne plus l'employer. La personne n'apparaît plus, au niveau de l'interface, dans la liste du personnel à qui la société va proposer des missions.

Dans ses observations en date du 7 décembre 2007, la société SIG a affirmé que le statut « *incident bloquant* » a été supprimé, tout en maintenant le statut « *incident majeur* » afin de pouvoir signaler les éventuels problèmes intervenus entre un client et son personnel. Lors de l'audience du 11 décembre 2007, la société SIG a affirmé que le statut « *inactif* » a également été retiré du système d'information et qu'elle réfléchissait sur les moyens de formaliser les statuts « *incident majeur* », en objectivant les commentaires pouvant être associés.

La Commission constate que la société n'a donc pas renoncé au statut « *incident majeur* » alors même qu'elle n'en a pas défini les critères d'inscription de ces incidents.

La CNIL observe que la société SIG n'a pas mis en place de procédures permettant d'indiquer ou de déterminer les critères objectifs permettant aux personnes, amenées à utiliser la base de données, de connaître les cas pour lesquels les statuts « *incident majeur* » doivent être inscrits dans les fiches du personnel.

La Commission considère par conséquent que la société SIG ne s'est pas conformée à la mise en demeure d'apporter toute justification (sensibilisation du personnel, contrôle réguliers du contenu des fichiers) permettant à la CNIL de considérer que les manquements constatés ne se reproduiront pas à l'avenir.

c) Lors de la mission de contrôle en date du 24 octobre 2007, la délégation de la CNIL a constaté qu'aucune procédure interne n'a été mise en œuvre au sein de la société SIG afin d'informer les employés des finalités du traitement au sein duquel sont enregistrées leurs données personnelles, et notamment les évaluations les concernant. De même, les intervenants n'étaient pas informés de l'existence des statuts « *incident majeur* », « *incident bloquant* » et « *inactif* ».

En effet, la CNIL a pu relever que les mentions prévues à l'article 32 de la loi du 6 janvier 1978 ne figurent ni sur les contrats intermittents à durée déterminée, qui représentent la majorité des contrats conclus, ni sur les formulaires de collecte de données utilisés pour le recrutement de personnel via le site Internet de la société. Ils ne sont pas plus affichés dans les locaux de la société SIG.

Dans ses observations écrites en date du 7 décembre 2007 et orales, prononcées lors de l'audience du 11 décembre 2007, la société SIG a également précisé qu'elle avait ajouté aux contrats d'embauche la mention : « *Conformément à la Loi informatique et Libertés du 6 janvier 1978, le salarié dispose d'un droit d'accès et de rectification pour toute information le concernant en s'adressant au siège social* ».

La société SIG a cependant précisé qu'elle réfléchissait à la mise en place d'une procédure interne permettant l'information des candidats à un emploi des finalités du traitement et des évaluations les concernant.

Dans ce conditions, la Commission estime que la société SIG ne s'est que partiellement conformée, sur ce point, à la mise en demeure qui lui a été adressée.

d) Lors de la mission de contrôle du 24 octobre 2007, la délégation de la CNIL a également constaté que les personnes ayant un statut « *inactif* » sont celles ne souhaitant plus travailler pour le compte de la société SIG, celles avec qui la société ne veut plus travailler à la suite de plusieurs « *incidents* » et celles ne travaillant plus depuis plus de 18 mois. Elles représentent 48 867 fiches de personnel pour un total de 68 127 personnes enregistrées dans la base « *KHEOPS* ».

Or, il apparaît que le fichier des personnes marquées du statut « *inactif* » contient des enregistrements des intervenants ne travaillant plus pour la société SIG depuis 1996.

De plus, une personne ayant le statut « *inactif* » peut être « réactivée » à tout moment dans la liste des personnes marquées du statut « *actif* », par le biais d'un traitement manuel des utilisateurs de l'outil de gestion du personnel de la société SIG.

Dans ses observations du 7 décembre 2007, la société SIG a précisé que les données à caractère personnel qu'elle traitait devaient être conservées pendant une durée minimale de 10 ans, afin de conserver la preuve de l'intervention de son personnel chez ses clients. Lors de l'audience du 11 décembre 2007, elle a également indiqué que le statut « *inactif* » a été supprimé de l'application « KHEOPS » et qu'elle réfléchissait sur la définition d'une durée de conservation ainsi que sur la mise en place d'une politique d'archivage.

La Commission considère qu'à ce jour aucune durée de conservation n'a été définie par la société SIG, s'agissant du traitement ayant pour finalité la gestion du personnel, puisqu'elle n'a déterminé qu'une durée minimale de conservation sans apporter de limite dans le temps ni d'explication justifiant une durée de 10 ans. S'agissant de la politique d'archivage, elle n'est qu'au stade de projet.

La Commission estime par conséquent que la société SIG ne s'est pas non plus conformée à la mise en demeure de la CNIL de définir une durée de conservation adéquate et proportionnée à la finalité du traitement.

5. Dans la proposition de sanction, le rapporteur a considéré que la société SIG était de mauvaise foi dans la mesure où les éléments communiqués par la société SIG, dans le courrier adressé le 10 septembre 2007 à la CNIL, sont en contradiction avec ce qui a pu être constaté lors de la mission de contrôle du 24 octobre 2007. En soutenant qu'elle s'était conformée aux dispositions de la loi du 6 janvier 1978 modifiée et en indiquant avoir abandonné l'application « SEP-SI » au profit du

système automatisé de gestion du personnel, initialement mis en œuvre par la société B&W Marketing, le rapporteur a estimé que la société SIG a délibérément apporté des réponses erronées à la mise en demeure adoptée par la Commission le 10 juillet 2007 et a sciemment souhaité maintenir l'opacité de sa situation.

La société SIG, tant dans ses observations écrites du 7 décembre 2007 que lors de l'audience du 11 décembre 2007, a indiqué la situation dans laquelle elle se trouvait lorsqu'elle a répondu à la mise en demeure, notamment la fusion avec la société B&W Marketing et les conséquences que cela a engendré.

Il a été, en revanche, décidé par la formation restreinte de ne pas retenir la mauvaise foi.

En conséquence, la Commission décide de faire application des dispositions des articles 45 et suivants de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer à l'encontre de la société SIG, sise 32-36 avenue de l'Europe à Vélizy-Villacoublay (78), compte tenu de la gravité des manquements, une sanction pécuniaire de 40.000 euros (quarante mille euros), qui sera rendue publique.

Le président
Alex TÜRK

**Délibération n° 2008-029 du 31 janvier 2008 sanctionnant
la société FAC INTERNATIONAL**

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK ;

Etant aussi présents, M. François GIQUEL, vice-président, M. Guy ROSIER, vice-président délégué, Mlle Anne DEBET, membre, M. Bernard PEYRAT, membre et M. Hubert BOUCHET, membre ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2007-131 mettant en demeure la société IMPACT NET, adoptée par la Commission nationale de l'informatique et des libertés le 14 juin 2007 ;

Vu la décision n° 2007-035C en date du 7 mai 2007 du président de la Commission nationale de l'informatique et des libertés de procéder à une mission de contrôle auprès de la société FAC INTERNATIONAL ;

Vu le rapport de M. Emmanuel de GIVRY, commissaire, remis en mains propres le 14 décembre 2007 et par lettre recommandée avec accusé-réception le 19 décembre 2007, à la société FAC INTERNATIONAL et à son avocat, le 10 janvier 2008 ;

Vu les observations en réponse reçues par courrier le 21 janvier 2008 et les pièces déposées à

l'audience, le 31 janvier 2008 ;

Après avoir entendu, lors de l'audience du 31 janvier 2008, M. Emmanuel de GIVRY, commissaire, en son rapport et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations ;

Après avoir entendu, lors de l'audience du 31 janvier 2008, les observations orales de Maître LAUGIER, avocat et Monsieur S, directeur général de la société FAC INTERNATIONAL, ceux-ci ayant pris la parole en dernier.

2

Constate les faits suivants :

1. La Commission nationale de l'informatique et des libertés (ci-après « CNIL ») a été saisie d'une plainte d'une personne s'interrogeant sur les conditions dans lesquelles elle a été démarchée, en septembre 2006, par la société FAC INTERNATIONAL pour des services d'assurance destinés essentiellement à des ressortissants étrangers.

La Commission a adressé à la société FAC INTERNATIONAL un courrier en date du 14 novembre 2006, lui demandant d'indiquer par quel moyen et selon quels critères elle avait sélectionné les coordonnées de la plaignante et si elle avait mis en oeuvre un fichier, manuel ou informatisé, pour procéder aux opérations de sélection et d'envoi.

Dans une lettre en date du 24 novembre 2006, la société FAC INTERNATIONAL a affirmé à la CNIL que la plaignante n'avait pas été sollicitée « *par rapport à sa supposée appartenance ethnique à une communauté* » et a précisé que les données relatives aux prospects démarchés « *sont communiquées par des clients reçus dans nos locaux (famille ou relations etc.), des formules de parrainage, des présidents d'association, etc.* ». La société FAC INTERNATIONAL a ensuite souligné dans ce courrier qu'« *il est probable que [la requérante] ait été sollicitée de cette façon, mais nous n'avons jamais constitué de fichier quelconque a fortiori basé sur la couleur ou la religion etc., et ceci du fait de la législation en*

France » et, dans le même temps, a précisé ne pas faire appel « à des achats de fichiers extérieurs ».

En application de la décision n° 2007-035C en date du 7 mai 2007 du président de la CNIL, une délégation de la Commission a procédé à une mission de vérification sur place le 21 mai 2007 auprès de la société FAC INTERNATIONAL, sise 56 rue de Londres à Paris (75008), afin d'apprécier l'exactitude des éléments apportés par la société, relatifs à ses opérations de prospection.

Lors de la mission de contrôle, le 21 mai 2007, la délégation de la CNIL a pu constater que la société FAC INTERNATIONAL utilisait principalement un logiciel dénommé « Nov Assur 3 », qui lui permettait de gérer ses clients et les personnes qu'elle démarchait.

La Commission a également relevé que les opérations de prospection menées par la société FAC INTERNATIONAL s'effectuaient principalement à partir des données à caractère personnel qui lui ont été communiquées, soit par ses propres clients dans le cadre d'opérations de parrainage soit, plus rarement, par des associations regroupant des personnes d'origine étrangère. Les informations relatives aux personnes démarchées étaient alors intégrées dans le logiciel « Nov Assur 3 ».

Pour autant, la délégation de la CNIL a constaté que les données à caractère personnel de la plaignante – qui, selon la société FAC INTERNATIONAL, a pu être démarchée dans le cadre d'une opération de parrainage – n'étaient pas présentes dans le logiciel de gestion. Une requête effectuée dans cet outil à partir de la référence du courrier qui lui a été adressé (« Ref : 904069 ») renvoyait cependant à une fiche portant sur « Test mailing – noms africains », laquelle ne comportait aucune donnée à caractère personnel.

Après interrogation des salariés, il est apparu que la société FAC INTERNATIONAL avait acquis auprès de la société IMPACT NET, au cours de l'année 2006, un fichier dont le devis

3

est libellé comme suit : « *Location adresses postales FICHER B2C Etrangers (Afrique, Maghreb) en France* ».

Selon le chef de cellule de production de la société FAC INTERNATIONAL, ce fichier aurait été constitué par la société IMPACT NET à partir d'une sélection opérée sur la consonance des noms des personnes figurant dans une base annuaire afin d'en déduire leur origine étrangère, supposée ou réelle. Il a par ailleurs été précisé que ce fichier comprenait de nombreuses adresses erronées et, qu'ainsi, il n'aurait été utilisé qu'une seule fois.

La Commission a rappelé qu'au regard de l'article 3 de la loi du 6 janvier 1978 modifiée, la société FAC INTERNATIONAL est responsable de traitement, dans la mesure où elle a commandé et acheté le fichier d'adresses postales à la société IMPACT NET à des fins de prospection commerciale.

La CNIL a également observé que l'utilisation d'un fichier d'adresses postales, pour la prospection de produits d'assurance destinés principalement à des ressortissants étrangers, constitué à partir de l'analyse de la consonance des noms ou prénoms des personnes était susceptible d'être contraire à l'article 8 de la loi du 6 janvier 1978 modifiée qui interdit, sauf en cas de consentement écrit de la personne concernée, de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques des personnes.

La Commission a par ailleurs constaté que les opérations de prospection menées par la société FAC INTERNATIONAL durant l'année 2006 n'avaient pas fait l'objet des formalités préalables prévues par la loi.

En conséquence, la Commission a mis en demeure, par une délibération n° 2007-131 du 14 juin 2007, la société FAC INTERNATIONAL sise, 56 rue de Londres à Paris (75008), dans un délai de quinze jours à compter de la notification de la décision (le 30 juillet 2007) :

- de procéder à l'accomplissement des formalités préalables concernant les

traitements à vocation de prospection commerciale mis en oeuvre ;

- d'apporter tous éléments garantissant que les traitements qu'elle met en oeuvre ne portent pas sur des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques des personnes.

2. En réponse à la mise en demeure du 14 juin 2007, la société FAC INTERNATIONAL a adressé à la CNIL, le 31 juillet 2007, un courrier auquel elle a joint un exemple de prospectus qu'elle utilise dans le cadre de ses opérations de prospection afin de démontrer « *qu'il n'est mentionné nulle part de données à caractère personnel faisant apparaître les origines raciales ou ethniques* » des personnes. La société FAC INTERNATIONAL a également précisé qu'elle a effectué auprès de la Commission une déclaration normale relative à la gestion et à la prospection de contrats d'assurance.

3. Un rapport de sanction, proposé à la Commission, a été notifié à la société FAC INTERNATIONAL par huissier le 14 décembre 2007 et par lettre recommandée avec accusé-réception le 19 décembre 2007. Il ressortait des conclusions du rapporteur qu'un des deux manquements à la loi du 6 janvier 1978 modifiée, identifiés par la CNIL, demeurait à l'issue

4 des éléments apportés par la société FAC INTERNATIONAL. Le rapporteur a également retenu la mauvaise foi de la société.

Le 21 janvier 2008, par courrier, la société FAC INTERNATIONAL a adressé à la CNIL ses observations en réponse.

4. Dans sa proposition de sanction, le rapporteur de la CNIL a constaté que la société FAC INTERNATIONAL a déposé, le 8 août 2007, une déclaration normale relative à la prospection et à la gestion des contrats d'assurance et qu'elle s'est bien conformée à la mise en demeure sur ce point.

5. S'agissant du manquement à l'interdiction de traiter des données à caractère personnel qui

font apparaître, directement ou indirectement, les origines raciales ou ethniques des personnes, le rapporteur a, au vu des éléments contractuels relevés lors de la mission de contrôle en date du 21 mai 2007 effectuée auprès de la société FAC INTERNATIONAL, constaté que cette dernière a acheté en connaissance de cause un fichier qui contenait des adresses postales de personnes étrangères originaires d’Afrique et du Maghreb, figurant sur une base annuaire, qui auraient été sélectionnées à partir de la consonance de leurs nom et prénoms par la société IMPACT NET.

Dans ses observations écrites en date du 21 janvier 2008 et orales, au jour de l’audience, la société FAC INTERNATIONAL a rappelé ses procédures de recherche de prospects et a affirmé qu’elle ne constituait aucun fichier de personnes qui auraient été sélectionnées selon leurs origines raciales ou ethniques.

S’agissant plus précisément du fichier loué par la société IMPACT NET, la société FAC INTERNATIONAL a tout d’abord précisé que la facture, sur laquelle s’est fondé le rapporteur, mentionne une opération d’e-mailing et non une « *Location adresses postales FICHIER B2C Etrangers (Afrique, Maghreb)* », figurant sur le seul devis établi entre les deux sociétés.

La Commission considère que si l’objet « *Location adresses postales FICHIER B2C Etrangers (Afrique, Maghreb)* » du fichier concerné n’est effectivement inscrit que sur le devis, ce dernier vaut contrat dans la mesure où y figure la mention « *bon pour accord* » cachetée par la société FAC INTERNATIONAL, ainsi que sur les conditions générales de vente. Les deux cocontractants, les sociétés FAC INTERNATIONAL et IMPACT NET, ont en effet convenu de la chose et du prix, et l’offre et l’acceptation se sont ainsi rencontrées. La Commission observe que le devis de la société IMPACT NET stipule expressément que le règlement du fichier concerné est effectué « *100% à la commande* ». Il apparaît ainsi que la facture a été délivrée une fois la prestation conformément exécutée, au regard des éléments

convenus dans le devis. Le montant du fichier d'adresses postales est d'ailleurs identique entre le devis et la facture de la société IMPACT NET.

La société FAC INTERNATIONAL a ensuite reconnu, dans ses observations écrites et orales en réponse au rapport de sanction, avoir commandé et loué le fichier contesté auprès de la société IMPACT NET mais a précisé, d'une part, qu'il a été détruit et, d'autre part, qu'elle ne pouvait contrôler ni l'initiative prise par un de ses salariés d'acquiescer le fichier concerné, ni les activités de la société IMPACT NET

5

La Commission entend rappeler que le I de l'article 3 de la loi du 6 janvier 1978 modifiée précise qu'est responsable de traitement la personne qui détermine sa finalité et ses moyens. Or, si la société IMPACT NET a constitué un fichier à partir de données dont la collecte est contraire aux dispositions de la loi « informatique et libertés », c'est la société FAC INTERNATIONAL qui l'a acquis et utilisé. C'est cette dernière qui traite des données à caractère personnel faisant apparaître les origines raciales ou ethniques des personnes et est, à cet égard, responsable de traitement.

L'argument selon lequel la location du fichier aurait été initiée par un salarié de la société n'enlève en rien la qualité de responsable de traitement à la société FAC INTERNATIONAL. La Commission constate que la société FAC INTERNATIONAL a bien acquis et utilisé un fichier faisant apparaître, directement ou indirectement, les origines raciales ou ethniques des personnes et considère par conséquent qu'elle ne s'est pas conformée à la mise en demeure du 14 juin 2007 sur ce point.

6. Dans sa proposition de sanction, le rapporteur de la CNIL a considéré que la société FAC INTERNATIONAL était de mauvaise foi dans la mesure où, dans son premier courrier adressé le 24 novembre 2006 à la CNIL, elle a soutenu qu'elle ne faisait appel à aucun fichier extérieur s'agissant de ses opérations de prospection commerciale alors qu'elle avait acquis

un fichier d'adresses postales auprès de la société IMPACT NET.

Dans ses observations écrites et orales, la société FAC INTERNATIONAL a affirmé qu'elle n'avait pas sciemment souhaité maintenir l'opacité de sa situation quant au fichier concerné mais qu'il s'agissait d'une erreur dans la mesure où elle ne se souvenait plus l'avoir utilisé. Elle a rappelé avoir détruit le fichier d'adresses postales acquis auprès de la société IMPACT NET.

Le rapporteur a pris en considération ces éléments, lors de la l'audience, et a retiré de ses conclusions la mauvaise foi initialement retenue à l'encontre de la société FAC INTERNATIONAL.

Il a été décidé par la formation restreinte de la CNIL de ne pas retenir la mauvaise foi.

7. La société FAC INTERNATIONAL, dans ses observations écrites du 21 janvier 2008, a fait savoir à la Commission qu'une sanction pécuniaire d'un montant de 30.000 euros était disproportionnée, eu égard à son chiffre d'affaires. A ce titre, la société a produit de nombreux documents comptables en attestant.

La formation restreinte de la CNIL a tenu compte des informations communiquées par la société FAC INTERNATIONAL.

6

En conséquence, la Commission décide de faire application des dispositions des articles 45 et suivants de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer à l'encontre de la société FAC INTERNATIONAL, sise 56 rue de Londres à Paris (75008), compte tenu de la gravité des manquements, une sanction pécuniaire de 15.000 euros (quinze mille euros), qui sera rendue publique.

Le président

Alex TÜRK



Décision n° 2003-467 DC du 13 mars 2003



Décision n° 2003-467 DC

- Communiqué de presse
- Dossier complet et texte adopté sur le site de l'Assemblée nationale
- Dossier complet et texte adopté sur le site du Sénat
- Texte du projet de loi déposé
- Saisine par 60 sénateurs
- Saisine par 60 députés
- Observations du gouvernement
- 60 députés (réplique)
- 60 sénateurs (réplique)
- Dossier documentaire
- Commentaire aux cahiers
- Références doctrinales
- Décision n° 2003-467 DC du 13 mars 2003

Loi pour la sécurité intérieure

Le Conseil constitutionnel a été saisi, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi pour la sécurité intérieure, le 14 février 2003, par M. Claude ESTIER, Mme Michèle ANDRÉ, MM. Bernard ANGELS, Bertrand AUBAN, Robert BADINTER, Jean-Pierre BEL, Jacques BELLANGER, Mme Maryse BERGÉ-LAVIGNE, M. Jean BESSON, Mme Marie-Christine BLANDIN, M. Didier BOULAUD, Mmes Yolande BOYER, Claire-Lise CAMPION, M. Bernard CAZEAU, Mme Monique CERISIER-ben GUIGA, MM. Gilbert

CHABROUX, Michel CHARASSE, Raymond COURRIÈRE, Roland COURTEAU, Yves DAUGE, Marcel DEBARGE, Claude DOMEIZEL, Michel DREYFUS-SCHMIDT, Mme Josette DURRIEU, MM. Jean-Claude FRÉCON, Bernard FRIMAT, Charles GAUTIER, Jean-Pierre GODEFROY, Jean-Noël GUÉRINI, Claude HAUT, Mme Odette HERVIAUX, MM. André LABARRÈRE, Serge LAGAUCHE, Yves KRATTINGER, Louis LE PENSEC, André LEJEUNE, Jacques MAHÉAS, Jean-Yves MANO, François MARC, Jean-Pierre MASSERET, Marc MASSION, Gérard MIQUEL, Michel MOREIGNE, Jean-Marc PASTOR, Daniel PERCHERON, Jean-Claude PEYRONNET, Jean-François PICHERAL, Bernard PIRAS, Jean-Pierre PLANCADE, Mmes Danièle POURTAUD, Gisèle PRINTZ, MM. Daniel RAOUL, Paul RAOULT, Daniel REINER, Roger RINCHET, Gérard ROUJAS, Claude SAUNIER, Michel SERGENT, Jean-Pierre SUEUR, Michel TESTON, Jean-Marc TODESCHINI, Pierre-Yvon TRÉMEL, André VANTOMME, André VÉZINHET, Marcel VIDAL, Henri WEBER, Mme Nicole BORVO, M. Guy FISCHER, Mmes Marie-Claude BEAUDEAU, Marie-France BEAUFILS, Danielle BIDARD, MM. Robert BRET, Yves COUELLE, Mmes Annie DAVID, Michelle DEMESSINE, Evelyne DIDIER, MM. Thierry FOUCAUD, Gérard LE CAM, Mme Hélène LUC, MM. Roland MUZEAU, Jack RALITE, Ivan RENAR et Mme Odette TERRADE, sénateurs, et le 19 février 2003, par MM. Jean-Marc AYRAULT, M. Damien ALARY, Mme Sylvie ANDRIEUX-BACQUET, MM. Jean-Marie AUBRON, Jean-Paul BACQUET, Jean-Pierre BALLIGAND, Gérard BAPT, Claude BARTOLONE, Jacques BASCOU, Christian BATAILLE, Jean-Claude BATEUX, Jean-Claude BEAUCHAUD, Éric BESSON, Jean-Louis BIANCO, Jean-Pierre BLAZY, Serge BLISKO, Patrick BLOCHE, Jean-Claude BOIS, Maxime BONO, Augustin BONREPAUX, Jean-Michel BOUCHERON, Pierre BOURGUIGNON, Mme Danielle BOUSQUET, MM. François BROTTES, Jean-Christophe CAMBADÉLIS, Thierry CARCENAC, Christophe CARESCHE, Mme Martine CARILLON-COUVREUR, MM. Laurent CATHALA, Jean-Paul CHANTEGUET, Michel CHARZAT, Alain CLAEYS, Mme Marie-Françoise CLERGEAU, MM. Gilles COCQUEMPOT, Pierre COHEN, Mme Claude DARCIAUX, M. Michel DASSEUX, Mme Martine DAVID, MM. Marcel DEHOUX, Michel DELEBARRE, Bernard DEROSIER, Michel DESTOT, Marc DOLEZ, François DOSÉ, René DOSIÈRE, Julien DRAY, Tony DREYFUS, Pierre DUCOUT, Jean-Pierre DUFAU, Jean-Louis DUMONT, Jean-Paul DUPRÉ, Yves DURAND, Henri EMMANUELLI, Claude ÉVIN, Laurent FABIUS, Jacques FLOCH, Pierre FORGUES, Michel FRANÇAIX, Jean GAUBERT, Mmes Nathalie GAUTIER, Catherine GÉNISSON, MM. Jean GLAVANY, Gaétan GORCE, Alain GOURIOU, Mmes Elisabeth GUIGOU, Paulette GUINCHARD-KUNSTLER, M. David HABIB, Mme Danièle HOFFMAN-RISPAL, MM. François HOLLANDE, Jean-Louis IDIART, Mme Françoise IMBERT, MM. Serge JANQUIN, Jean-Pierre KUCHEIDA, Mme Conchita LACUEY, MM. Jérôme LAMBERT, François LAMY, Jack LANG, Jean LAUNAY, Jean-Yves LE BOUILLONNEC, Gilbert LE BRIS, Jean-Yves LE DÉAUT, Jean-Yves LE DRIAN, Jean LE GARREC, Jean-Marie LE GUEN, Bruno LE ROUX, Mme Marylise LEBRANCHU, MM. Michel LEFAIT, Patrick LEMASLE, Guy LENGAGNE, Mme Annick LEPETIT, MM. Jean-Claude LEROY, Michel LIEBGOTT, Mme Martine LIGNIÈRES-CASSOU, MM. François LONCLE, Victorin LUREL, Bernard MADRELLE, Philippe MARTIN, Christophe MASSE, Didier MATHUS, Kléber MESQUIDA, Jean MICHEL, Didier MIGAUD, Mme Hélène MIGNON, MM. Arnaud MONTEBOURG, Henri NAYROU, Alain NÉRI, Mme Marie-Renée OGET, MM. Michel PAJON, Christian PAUL, Germinal PEIRO, Jean-Claude PEREZ, Mmes Marie-Françoise PEROL-DUMONT, Geneviève PERRIN-GAILLARD, MM. Jean-Jack QUEYRANNE, Paul QUILÈS, Alain RODET, Bernard ROMAN, René ROUQUET, Patrick ROY, Mme Ségolène ROYAL, M. Michel SAINTE-MARIE, Mme Odile SAUGUES, MM. Henri SICRE, Dominique STRAUSS-KAHN, Pascal

TERRASSE, Philippe TOURTELIER, Daniel VAILLANT, André VALLINI, Manuel VALLS, Michel VERGNIER, Alain VIDALIES, Jean-Claude VIOLLET, Philippe VUILQUE, Mme Chantal ROBIN-RODRIGO, M. Simon RENUCCI, Mme Christiane TAUBIRA et M. Roger-Gérard SCHWARTZENBERG, députés ;
LE CONSEIL CONSTITUTIONNEL,

Vu la Constitution ;
Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel, notamment le chapitre II du titre II de ladite ordonnance ;
Vu la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 ;
Vu le code pénal ;
Vu le code de procédure pénale ;
Vu le code général des collectivités territoriales ;
Vu le code de justice administrative ;
Vu le code des communes applicable en Nouvelle-Calédonie ;
Vu la loi du 12 avril 1906 modifiant les articles 66, 67 du code pénal, 340 du code d'instruction criminelle et fixant la majorité pénale à l'âge de dix-huit ans ;
Vu la loi du 22 juillet 1912 sur les tribunaux pour enfants et adolescents et sur la liberté surveillée ;
Vu l'ordonnance n° 45-174 du 2 février 1945 relative à l'enfance délinquante ;
Vu l'ordonnance n° 45-2658 du 2 novembre 1945 modifiée relative aux conditions d'entrée et de séjour des étrangers en France ;
Vu la loi n° 77-1460 du 29 décembre 1977 modifiant le régime communal dans le territoire de la Polynésie française ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 2 et 39 ;
Vu la loi n° 79-587 du 11 juillet 1979 modifiée relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public, notamment son article 1er ;
Vu la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de surveillance, de gardiennage et de transport de fonds ;
Vu la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité ;
Vu la loi n° 98-349 du 11 mai 1998 relative à l'entrée et au séjour des étrangers en France et au droit d'asile ;
Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, notamment son article 24 ;
Vu la loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes ;
Vu la loi n° 2000-614 du 5 juillet 2000 relative à l'accueil et à l'habitat des gens du voyage ;
Vu la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ;
Vu la loi n° 2002-307 du 4 mars 2002 complétant la loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence

et les droits des victimes ;
 Vu la loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure ;
 Vu les observations du Gouvernement, enregistrées le 3 mars 2003 ;
 Vu les observations en réplique présentées par les sénateurs auteurs de la première saisine, enregistrées le 11 mars 2003 ;
 Vu les observations en réplique présentées par les députés auteurs de la seconde saisine, enregistrées le 11 mars 2003 ;
 Le rapporteur ayant été entendu ;

1. Considérant que les auteurs des deux saisines défèrent au Conseil constitutionnel la loi pour la sécurité intérieure ; qu'ils contestent notamment la conformité à la Constitution de ses articles 3, 11, 12, 13, 21, 25, 28, 30, 50, 51, 53, 64, 65, 75, 76, 96, 113, 122, 123, 141 et 142 ;

- SUR L'ARTICLE 3

2. Considérant que l'article 3 de la loi déferée complète l'article L. 2215-1 du code général des collectivités territoriales par un 4° relatif aux pouvoirs de réquisition conférés au préfet en vue de rétablir l'ordre public ; qu'aux termes du premier alinéa de ce 4° : " En cas d'urgence, lorsque l'atteinte au bon ordre, à la salubrité, à la tranquillité et à la sécurité publiques l'exige et que les moyens dont dispose le préfet ne permettent plus de poursuivre les objectifs pour lesquels il détient des pouvoirs de police, celui-ci peut, par arrêté motivé, pour toutes les communes du département ou plusieurs ou une seule d'entre elles, réquisitionner tout bien et service, requérir toute personne nécessaire au fonctionnement de ce service ou à l'usage de ce bien et prescrire toute mesure utile jusqu'à ce que l'atteinte à l'ordre public ait pris fin " ; qu'en vertu de son deuxième alinéa, cet arrêté doit être motivé et fixer la nature des prestations requises, la durée de la mesure de réquisition, ainsi que les modalités de son application ; que son troisième alinéa dispose que le préfet peut faire exécuter d'office les mesures prescrites par son arrêté ; que les quatre alinéas suivants sont relatifs à la rétribution due par l'Etat aux personnes requises ; qu'aux termes du huitième alinéa : " En cas d'inexécution volontaire par la personne requise des obligations qui lui incombent en application de l'arrêté édicté par le préfet, le président du tribunal administratif ou le magistrat qu'il délègue peut, sur demande de l'autorité requérante, prononcer une astreinte dans les conditions prévues aux articles L. 911-6 à L. 911-8 du code de justice administrative " ; qu'enfin, le dernier alinéa dispose que " Le refus d'exécuter les mesures prescrites par l'autorité requérante constitue un délit qui est puni de six mois d'emprisonnement et de 10 000 euros d'amende " ;

3. Considérant que les auteurs des deux saisines reprochent à cette disposition d'être rédigée en termes trop généraux et imprécis pour satisfaire aux exigences de l'article 34 de la Constitution, alors même que les pouvoirs qu'elle confère au préfet seraient susceptibles d'affecter l'exercice des libertés publiques ; qu'il en serait ainsi en particulier de la formule : " prescrire toute mesure utile jusqu'à ce que l'atteinte à l'ordre public ait pris fin " ; que la disposition contestée serait en outre, selon eux, contraire au principe de nécessité des peines, dès lors que l'astreinte prononcée par le tribunal administratif, en cas d'inexécution volontaire par la personne requise des obligations lui incombant en vertu de l'arrêté préfectoral, pourra se cumuler avec la sanction pénale prévue en cas d'inexécution des mesures prescrites par l'autorité requérante ;

4. Considérant, en premier lieu, que les dispositions contestées tendent à préciser et à compléter les pouvoirs de police administrative appartenant d'ores et déjà à l'autorité préfectorale en cas d'urgence, lorsque le rétablissement de l'ordre public exige des mesures de réquisition ; qu'en apportant les précisions et compléments en cause, le législateur n'est pas resté en deçà de sa compétence ; qu'en outre, les mesures prises par le préfet, sur le fondement de ces dispositions, pourront être contestées par les intéressés devant le juge administratif, notamment dans le cadre d'un référé ou d'une procédure d'astreinte ;
5. Considérant, en second lieu, que l'astreinte dont le principe est institué par les dispositions précitées a pour finalité de contraindre la personne qui s'y refuse à exécuter les obligations auxquelles l'arrêté de réquisition la soumet ; qu'elle ne saurait être regardée comme une peine ou une sanction au sens de l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789 ; que, par suite, les moyens tirés de la violation des principes de nécessité des peines et de non-cumul des peines pour une même faute doivent être écartés comme inopérants ;
- SUR LES ARTICLES 11 A 13 :
6. Considérant que ces articles prévoient de nouvelles modalités de visite des véhicules par les officiers de police judiciaire et les agents placés sous leur contrôle ; que les auteurs des deux saisines reprochent à ces articles de porter des atteintes excessives au respect de la vie privée, à l'inviolabilité du domicile, à la liberté d'aller et venir et à la liberté individuelle ; que, selon eux, ils font une place insuffisante au juge judiciaire, gardien de la liberté individuelle, dans le déroulement de la procédure ; que les articles critiqués seraient enfin entachés d'une incompétence négative en raison de l'imprécision qui affecterait leur formulation ;
- Quant aux normes constitutionnelles applicables à la visite des véhicules :
7. Considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 : " Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression " ; que son article 4 proclame que " La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi " ; qu'en vertu de l'article 66 de la Constitution : " Nul ne peut être arbitrairement détenu. - L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi " ;
8. Considérant qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté d'aller et venir et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789, ainsi que la liberté individuelle, que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire ;
9. Considérant que les mesures de police administrative susceptibles d'affecter l'exercice des libertés constitutionnellement garanties doivent être justifiées par la nécessité de sauvegarder l'ordre public ;
10. Considérant que, en dehors des cas où ils agissent sur réquisition de l'autorité judiciaire, les agents habilités ne peuvent disposer d'une

personne que lorsqu'il y a des raisons plausibles de soupçonner qu'elle vient de commettre une infraction ou lorsqu'il y a des motifs raisonnables de croire à la nécessité de l'empêcher d'en commettre une ; qu'en pareil cas, l'autorité judiciaire doit en être au plus tôt informée et le reste de la procédure placé sous sa surveillance ;
 - Quant à l'article 11 :

11. Considérant que l'article 11 rétablit dans le code de procédure pénale un article 78-2-2 ainsi rédigé : " Sur réquisitions écrites du procureur de la République aux fins de recherche et de poursuite des actes de terrorisme visés par les articles 421-1 à 421-5 du code pénal, des infractions en matière d'armes et d'explosifs visées par l'article 3 de la loi du 19 juin 1871 qui abroge le décret du 4 septembre 1870 sur la fabrication des armes de guerre et par les articles 20, 31 et 32 du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, des infractions de vol visées par les articles 311-3 à 311-11 du code pénal, de recel visées par les articles 321-1 et 321-2 du même code ou des faits de trafic de stupéfiants visés par les articles 222-34 à 222-38 dudit code, les officiers de police judiciaire, assistés, le cas échéant, des agents de police judiciaire et des agents de police judiciaire adjoints mentionnés aux 1°, 1° bis et 1° ter de l'article 21 peuvent, dans les lieux et pour la période de temps que ce magistrat détermine et qui ne peut excéder vingt-quatre heures, renouvelables sur décision expresse et motivée selon la même procédure, procéder non seulement aux contrôles d'identité prévus au sixième alinéa de l'article 78-2 mais aussi à la visite des véhicules circulant, arrêtés ou stationnant sur la voie publique ou dans des lieux accessibles au public. - Pour l'application des dispositions du présent article, les véhicules en circulation ne peuvent être immobilisés que le temps strictement nécessaire au déroulement de la visite qui doit avoir lieu en présence du conducteur. Lorsqu'elle porte sur un véhicule à l'arrêt ou en stationnement, la visite se déroule en présence du conducteur ou du propriétaire du véhicule ou, à défaut, d'une personne requise à cet effet par l'officier ou l'agent de police judiciaire et qui ne relève pas de son autorité administrative. La présence d'une personne extérieure n'est toutefois pas requise si la visite comporte des risques graves pour la sécurité des personnes et des biens. - En cas de découverte d'une infraction ou si le conducteur ou le propriétaire du véhicule le demande ainsi que dans le cas où la visite se déroule en leur absence, il est établi un procès-verbal mentionnant le lieu et les dates et heures du début et de la fin de ces opérations. Un exemplaire en est remis à l'intéressé et un autre est transmis sans délai au procureur de la République. - Toutefois, la visite des véhicules spécialement aménagés à usage d'habitation et effectivement utilisés comme résidence ne peut être faite que conformément aux dispositions relatives aux perquisitions et visites domiciliaires. - Le fait que ces opérations révèlent des infractions autres que celles visées dans les réquisitions du procureur de la République ne constitue pas une cause de nullité des procédures incidentes " ;

12. Considérant, s'agissant de visites de véhicules réalisées sur réquisitions du procureur de la République, que la conciliation assurée par ces dispositions entre les principes constitutionnels rappelés ci-dessus n'est entachée d'aucune erreur manifeste ; que la liste des infractions figurant au premier alinéa du nouvel article 78-2-2 du code de procédure pénale n'est pas manifestement excessive au regard de l'intérêt public qui s'attache à la recherche des auteurs de ces infractions ; que ces dispositions ne méconnaissent pas l'article 66 de la Constitution ; que leurs termes sont assez clairs et précis pour répondre aux exigences de l'article 34 de celle-ci ; qu'il en est notamment ainsi, contrairement aux affirmations des requérants, de l'expression " lieux accessibles au public " et de celle de " véhicules spécialement aménagés à usage d'habitation et effectivement utilisés comme résidence " ; qu'ainsi qu'il ressort des termes mêmes du premier alinéa du

nouvel article 78-2-2 du code de procédure pénale, chaque renouvellement de l'autorisation du procureur de la République vaudra pour une durée de vingt-quatre heures ;
 - Quant à l'article 12 :

13. Considérant que l'article 12 de la loi déferée insère dans le code de procédure pénale un article 78-2-3 ainsi rédigé : " Les officiers de police judiciaire, assistés, le cas échéant, des agents de police judiciaire et des agents de police judiciaire adjoints mentionnés aux 1°, 1° bis et 1° ter de l'article 21, peuvent procéder à la visite des véhicules circulant ou arrêtés sur la voie publique ou dans des lieux accessibles au public lorsqu'il existe à l'égard du conducteur ou d'un passager une ou plusieurs raisons plausibles de soupçonner qu'il a commis, comme auteur ou comme complice, un crime ou un délit flagrant ; ces dispositions s'appliquent également à la tentative. - Les dispositions des deuxième, troisième et quatrième alinéas de l'article 78-2-2 sont applicables aux dispositions du présent article " ;

14. Considérant, s'agissant des visites de véhicules réalisées en vue de constater des infractions flagrantes, que ces dispositions sont conformes aux exigences constitutionnelles ci-dessus rappelées en raison de la condition à laquelle elles subordonnent les visites ; qu'elles ne méconnaissent pas l'article 66 de la Constitution ; qu'elles sont formulées en termes assez clairs et précis pour respecter la mission confiée au législateur par l'article 34 de celle-ci ;
 - Quant à l'article 13 :

15. Considérant que l'article 13 de la loi déferée insère dans le code de procédure pénale un article 78-2-4 ainsi rédigé : " Pour prévenir une atteinte grave à la sécurité des personnes et des biens, les officiers de police judiciaire et, sur l'ordre et sous la responsabilité de ceux-ci, les agents de police judiciaire et les agents de police judiciaire adjoints mentionnés aux 1°, 1° bis, 1° ter de l'article 21 peuvent procéder non seulement aux contrôles d'identité prévus au septième alinéa de l'article 78-2 mais aussi, avec l'accord du conducteur ou, à défaut, sur instructions du procureur de la République communiquées par tous moyens, à la visite des véhicules circulant, arrêtés ou stationnant sur la voie publique ou dans des lieux accessibles au public. - Dans l'attente des instructions du procureur de la République, le véhicule peut être immobilisé pour une durée qui ne peut excéder trente minutes. - Les deuxième, troisième et quatrième alinéas de l'article 78-2-2 sont applicables aux dispositions du présent article " ;

16. Considérant, s'agissant des visites de véhicules réalisées dans le cadre de la police administrative, que ces dispositions satisfont aux exigences constitutionnelles rappelées ci-dessus en raison de la condition à laquelle elles subordonnent ces visites ; qu'elles ne méconnaissent pas l'article 66 de la Constitution ; qu'elles sont formulées en termes assez clairs et précis pour respecter la mission confiée au législateur par l'article 34 de celle-ci ;
 - SUR LES ARTICLES 21 ET 25 :

17. Considérant que ces articles portent sur les traitements automatisés de données nominatives mis en oeuvre par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions ;

18. Considérant qu'il est soutenu par les auteurs des deux saisines que les dispositions contestées porteraient atteinte au respect de la vie privée ; qu'en renvoyant au pouvoir réglementaire le soin de fixer certaines caractéristiques desdits traitements, en particulier la durée de conservation des données, le législateur n'aurait pas épuisé sa compétence ; que certaines utilisations seraient sans lien avec la finalité

des traitements ; qu'en particulier, en permettant la consultation des données nominatives à des fins d'enquête administrative, le législateur permettrait qu'il en soit fait un usage préjudiciable aux droits des personnes concernées ; que seraient méconnus le principe fondamental reconnu par les lois de la République en matière de droit pénal des mineurs ainsi que la présomption d'innocence et le principe d'égalité ;

- Quant aux normes constitutionnelles applicables :

19. Considérant que la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le respect de la vie privée ;

20. Considérant qu'il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il lui appartient notamment d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés ;

- Quant au respect de la vie privée :

21. Considérant que le I de l'article 21 prévoit que : " Les services de la police nationale et de la gendarmerie nationale peuvent mettre en oeuvre des applications automatisées d'informations nominatives recueillies au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'Etat, afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs " ; qu'aux termes du II du même article : " Les traitements mentionnés au I peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au premier alinéa du I. - Ils peuvent également contenir des informations sur les victimes de ces infractions ; ces dernières peuvent toutefois s'opposer à ce que les informations nominatives les concernant soient conservées dans le fichier dès lors que l'auteur des faits a été définitivement condamné " ;

22. Considérant que le III de l'article 21 place le traitement des informations nominatives sous le contrôle du procureur de la République compétent ; que celui-ci peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire ; que la rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande ; qu'en cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention ; que les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles ;

23. Considérant que le IV de l'article 21 définit strictement les personnes, autres que les magistrats judiciaires, habilitées, en raison de leurs attributions de police judiciaire, à utiliser les traitements en cause ; qu'en vertu du V du même article : " Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article. Il précise notamment la liste des contraventions mentionnées au I, la durée de conservation des informations enregistrées, les modalités

d'habilitation des personnes mentionnées au IV ainsi que, le cas échéant, les conditions dans lesquelles les personnes intéressées peuvent exercer leur droit d'accès " ;

24. Considérant que l'article 22 de la loi déferée, qui modifie l'article 39 de la loi du 6 janvier 1978 susvisée, fixe les conditions et modalités selon lesquelles les données nominatives contenues dans les fichiers intéressant en particulier la sécurité publique peuvent être communiquées aux personnes intéressées ;

25. Considérant que l'article 23 dresse limitativement la liste des décisions judiciaires au titre desquelles une personne peut être inscrite dans le fichier des personnes recherchées ;

26. Considérant, enfin, ainsi qu'il ressort des débats parlementaires, que la loi du 6 janvier 1978 susvisée, que le législateur n'a pas entendu écarter, s'appliquera aux traitements en cause ;

27. Considérant que l'ensemble de ces garanties est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée ;

- Quant à l'utilisation des traitements à des fins administratives ;

28. Considérant que l'article 25 ne permet la consultation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire que pour des finalités déterminées ;

29. Considérant qu'il s'agit, en premier lieu, " des décisions de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux " ; qu'en pareil cas, la consultation a pour but exclusif de vérifier que le comportement des intéressés n'est pas incompatible avec l'exercice des fonctions ou missions envisagées ; qu'elle s'effectue dans la stricte mesure exigée par la protection de la sécurité des personnes et par la défense des intérêts fondamentaux de la Nation ; qu'elle donne lieu à information des intéressés ; qu'un décret en Conseil d'Etat doit fixer la liste des enquêtes administratives qui, en application de l'article 25 de la loi déferée, pourront donner lieu à la consultation des traitements automatisés d'informations personnelles mentionnés à son article 21 ;

30. Considérant que la consultation est également prévue " pour l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux " ; qu'en pareil cas, la consultation est faite par des agents de la police et de la gendarmerie spécialement habilités à cet effet ou, dans des conditions déterminées par décret en Conseil d'Etat, par des personnels investis de missions de police administrative désignés selon les mêmes procédures ;

31. Considérant que la consultation est enfin permise pour " l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations

prioritaires de défense visés à l'article 17 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense " ; qu'en pareil cas, la consultation est effectuée par des agents de la police et de la gendarmerie nationale spécialement habilités à cet effet ;

32. Considérant qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées ;

33. Considérant qu'eu égard aux motifs qu'elle fixe pour ces consultations, comme aux restrictions et précautions dont elle les assortit, la loi déferée ne méconnaît par elle-même aucune des exigences constitutionnelles ci-dessus mentionnées ;

34. Considérant, en outre, qu'en vertu de l'article 2 de la loi du 6 janvier 1978 susvisée, que ne remettent pas en cause les dispositions contestées : " Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé " ; que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative ;

35. Considérant, enfin, que ces dispositions ne portent pas par elles-mêmes atteinte aux droits des étrangers, lesquels ne comprennent aucun droit de caractère général et absolu d'acquérir la nationalité française ou de voir renouveler leur titre de séjour ; qu'elles ne sauraient en revanche être entendues comme remettant en cause l'acquisition de la nationalité française lorsque celle-ci est, en vertu de la loi, de plein droit, ni le renouvellement d'un titre de séjour lorsque celui-ci est, en vertu de la loi, de plein droit ou lorsqu'il est commandé par le respect du droit de chacun à mener une vie familiale normale ;

- Quant au principe fondamental reconnu par les lois de la République en matière de droit pénal des mineurs :

36. Considérant que l'atténuation de la responsabilité pénale des mineurs en fonction de l'âge, comme la nécessité de rechercher leur relèvement éducatif et moral par des mesures adaptées à leur âge et à leur personnalité, prononcées par une juridiction spécialisée ou selon des procédures appropriées, ont été constamment reconnues par les lois de la République depuis le début du vingtième siècle ; que ces principes trouvent notamment leur expression dans la loi du 12 avril 1906 sur la majorité pénale des mineurs, la loi du 22 juillet 1912 sur les tribunaux pour enfants et l'ordonnance du 2 février 1945 sur l'enfance délinquante ;

37. Considérant que ce principe n'est pas méconnu du seul fait que les dispositions contestées ne comportent pas de limitation quant à l'âge des personnes sur lesquelles sont recueillies des informations dans les conditions prévues à l'article 21 de la loi déferée ;

38. Considérant toutefois qu'il appartiendra au décret prévu au V de l'article 21 de la loi déferée de déterminer une durée de conservation conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants ;

- Quant au respect de la présomption d'innocence :

39. Considérant qu'aux termes de l'article 9 de la Déclaration de 1789 : " Tout homme étant présumé innocent, jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être

sévèrement réprimé par la loi " ;

40. Considérant, en premier lieu, que l'enregistrement de données nominatives dans des traitements de la nature de ceux auxquels fait référence l'article 21 de la loi déferée ne porte par lui-même aucune atteinte au principe de la présomption d'innocence ;

41. Considérant, en deuxième lieu, qu'en cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées ; que, si le procureur de la République peut en prescrire le maintien " pour des raisons liées à la finalité du fichier ", cette exception à la règle générale d'effacement ne peut être justifiée que par des nécessités d'ordre public appréciées par l'autorité judiciaire ; qu'il est alors fait mention de la décision de relaxe ou d'acquiescement dans le fichier ;

42. Considérant, en troisième lieu, qu'en cas de décision de non lieu ou de classement sans suite, les données personnelles concernant les personnes mises en cause sont conservées sauf si le procureur de la République en ordonne l'effacement ; que, s'il ne le fait pas, les décisions de non lieu et, lorsqu'ils sont motivés par une insuffisance de charges, les classements sans suite font l'objet d'une mention dans le fichier ; qu'il appartiendra ainsi à l'autorité judiciaire d'apprécier dans chaque cas, compte tenu des motifs de la décision prise, si les nécessités de l'ordre public justifient ou non le maintien des données en cause ;

43. Considérant, enfin, ainsi qu'il a été dit ci-dessus, que toute personne inscrite dans le fichier devra pouvoir exercer son droit d'accès et de rectification des données la concernant dans les conditions prévues par l'article 39 de la loi du 6 janvier 1978 susvisée ;

- Quant au principe d'égalité :

44. Considérant qu'en vertu du II de l'article 21, la victime peut s'opposer au maintien dans le fichier des informations nominatives la concernant dès lors que l'auteur des faits a été définitivement condamné ; que les sénateurs requérants ne sauraient invoquer utilement, à l'encontre de cette disposition, une quelconque rupture du principe d'égalité ;

- Quant à la compétence du législateur :

45. Considérant que, loin d'avoir méconnu l'étendue de sa compétence, le législateur a assorti les dispositions critiquées de précisions dont certaines relèvent du pouvoir réglementaire et qui, au demeurant, avaient jusqu'ici été traitées comme telles ;

46. Considérant qu'il résulte de tout ce qui précède que, sous les réserves énoncées aux considérants 26, 34, 35, 38 et 43, les articles 21 et 25 ne sont pas contraires à la Constitution ;

- SUR L'ARTICLE 28 :

47. Considérant que l'article 28 insère dans le code de procédure pénale un article 706-47-1 ; qu'aux termes des trois premiers alinéas du nouvel article : " L'officier de police judiciaire, agissant au cours de l'enquête ou sur commission rogatoire, peut faire procéder sur toute personne contre laquelle il existe des indices graves ou concordants d'avoir commis un viol, une agression sexuelle ou une atteinte sexuelle prévus par les articles 222-23 à 222-26 et 227-25 à 227-27 du code pénal, à un examen médical et à une prise de sang afin de déterminer si cette personne n'est pas atteinte d'une maladie sexuellement transmissible. - Le médecin, l'infirmier ou la personne habilitée par les dispositions du code de la santé publique à effectuer les actes réservés à ces professionnels, qui est requis à cette fin par l'officier de police judiciaire, doit s'efforcer d'obtenir le consentement de l'intéressé. - A la demande de la victime ou lorsque son intérêt le justifie, cette opération peut être effectuée sans le consentement de l'intéressé sur instructions écrites du procureur de la République ou du juge

d'instruction qui sont versées au dossier de la procédure " ; que le quatrième alinéa du nouvel article 706-47-1 prévoit que le résultat du dépistage est porté à la connaissance de la victime par l'intermédiaire d'un médecin ; que son cinquième alinéa punit le refus de se soumettre au dépistage ;

48. Considérant que, pour les auteurs des deux saisines, ces dispositions méconnaîtraient les articles 8 et 9 de la Déclaration de 1789 en raison de la liste d'infractions dressée, selon eux, de façon trop extensive par le premier alinéa du nouvel article 706-47-1 du code de procédure pénale ; que l'obligation d'un examen médical et d'une prise de sang serait excessive au stade de l'enquête préliminaire ; que rien ne justifierait qu'un prélèvement sanguin soit effectué à la demande de la victime sans le consentement de l'intéressé ; que, s'agissant d'une atteinte à la liberté individuelle, l'autorité judiciaire ne saurait, selon la saisine, se borner à ratifier la demande de la victime ; que l'obligation de se soumettre à un examen médical et à une prise de sang méconnaîtrait les droits de la défense, le principe du procès équitable et " l'égalité des armes " entre l'auteur et la victime ;

49. Considérant, en premier lieu, que les dispositions critiquées prévoient, dans l'intérêt de la victime d'un viol, d'une agression ou d'une atteinte sexuelle, la possibilité de procéder à un simple examen médical et à un simple prélèvement sanguin sur une personne à l'encontre de laquelle il existe des indices graves ou concordants d'avoir commis l'un des actes mentionnés aux articles 222-23 à 222-26 et 227-25 à 227-27 du code pénal ; qu'à défaut de consentement de l'intéressé, l'opération ne peut être pratiquée que sur instructions écrites du procureur de la République ou du juge d'instruction, et seulement à la demande de la victime ou lorsque son intérêt le justifie, notamment, dans cette dernière hypothèse, lorsque la victime est mineure ; que, dans ces conditions, la contrainte à laquelle est soumise la personne concernée n'entraîne aucune rigueur qui ne serait pas nécessaire au regard des autres exigences constitutionnelles en cause et, plus particulièrement, conformément au onzième alinéa du Préambule de la Constitution de 1946, de la protection de la santé de la victime ; que l'examen médical et le prélèvement sanguin ne portent atteinte ni aux droits de la défense, ni aux exigences du procès équitable, ni à la présomption d'innocence ;

50. Considérant, en deuxième lieu, que la liste des infractions fixée au premier alinéa du nouvel article 706-47-1 du code de procédure pénale n'est entachée d'aucune erreur manifeste eu égard à l'objectif que s'est assigné le législateur ;

51. Considérant, enfin, qu'il résulte des termes mêmes du troisième alinéa du nouvel article 706-47-1 du code de procédure pénale que l'autorité judiciaire disposera de toute latitude d'appréciation lorsque la victime demandera que soit pratiqué un examen médical ou un prélèvement sanguin nonobstant le refus de l'intéressé ; qu'elle pourra en particulier, lorsque la nature de l'infraction ne comporte pas de risque pour la santé de la victime, ne pas donner suite à la demande de celle-ci ;

- SUR L'ARTICLE 30 :

52. Considérant que cet article insère notamment dans le code de procédure pénale un article 55-1 ainsi rédigé : " L'officier de police judiciaire peut procéder, ou faire procéder sous son contrôle, sur toute personne susceptible de fournir des renseignements sur les faits en cause ou sur toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre l'infraction, aux opérations de prélèvements externes nécessaires à la réalisation d'examens techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête. - Il procède, ou fait procéder sous son contrôle, aux

opérations de signalisation nécessaires à l'alimentation et à la consultation des fichiers de police selon les règles propres à chacun de ces fichiers. - Le refus de se soumettre aux opérations de prélèvement ordonnées par l'officier de police judiciaire est puni d'un an d'emprisonnement et de 15 000 euros d'amende ;

53. Considérant que les députés requérants font valoir que ces dispositions sont imprécises ; qu'elles portent atteinte à la liberté individuelle et à l'inviolabilité du corps humain ; qu'en soumettant aux opérations de prélèvement toute " personne susceptible de fournir des renseignements ", elles méconnaissent la présomption d'innocence ; que la peine prévue en cas de refus de se soumettre au prélèvement est disproportionnée ;

54. Considérant que les dispositions contestées sont formulées en termes assez clairs et précis pour satisfaire aux prescriptions de l'article 34 de la Constitution ; que les " personnes susceptibles de fournir des renseignements sur les faits en cause " sont celles qui sont déjà tenues de comparaître devant l'officier de police judiciaire en vertu de l'article 62 du code de procédure pénale ; qu'il résulte des dispositions de l'article 706-54 du code de procédure pénale, dans sa rédaction issue de l'article 29 de la loi déferée, que les empreintes génétiques de ces personnes ne pourront en aucun cas être enregistrées, ni donc a fortiori conservées, dans le fichier national automatisé des empreintes génétiques ; que, dans ces conditions, lesdites personnes ne sont ni définies de façon trop imprécise, ni soumises, du fait de l'obligation nouvelle que leur impose l'article contesté, à une rigueur non nécessaire au sens de l'article 9 de la Déclaration de 1789 ;

55. Considérant, ainsi qu'il ressort de ses termes mêmes, éclairés par les débats parlementaires, que l'expression " prélèvement externe " fait référence à un prélèvement n'impliquant aucune intervention corporelle interne ; qu'il ne comportera donc aucun procédé douloureux, intrusif ou attentatoire à la dignité des intéressés ; que manque dès lors en fait le moyen tiré de l'atteinte à l'inviolabilité du corps humain ; que le prélèvement externe n'affecte pas davantage la liberté individuelle de l'intéressé ; qu'enfin, le prélèvement étant effectué dans le cadre de l'enquête et en vue de la manifestation de la vérité, il n'impose à la " personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre l'infraction " aucune rigueur qui ne serait pas nécessaire ;

56. Considérant que les prélèvements externes ne portent pas atteinte à la présomption d'innocence ; qu'ils pourront, au contraire, établir l'innocence des personnes qui en sont l'objet ;

57. Considérant, enfin, qu'en l'absence de voies d'exécution d'office du prélèvement et compte tenu de la gravité des faits susceptibles d'avoir été commis, le législateur n'a pas fixé un quantum disproportionné pour le refus de prélèvement ; qu'il appartiendra toutefois à la juridiction répressive, lors du prononcé de la peine sanctionnant ce refus, de proportionner cette dernière à celle qui pourrait être infligée pour le crime ou le délit à l'occasion duquel le prélèvement a été demandé ; que, sous cette réserve, l'article 30 n'est pas contraire à la Constitution ;

- SUR L'ARTICLE 50 :

58. Considérant que cet article insère dans le code pénal un article 225-10-1 ainsi rédigé : " Le fait, par tout moyen, y compris par une attitude même passive, de procéder publiquement au racolage d'autrui en vue de l'inciter à des relations sexuelles en échange d'une rémunération ou d'une promesse de rémunération est puni de deux mois d'emprisonnement et de 3 750 euros d'amende " ; qu'il complète en outre l'article 225-12-1 du même code par un alinéa aux termes duquel : " Est puni des mêmes peines le fait de solliciter, d'accepter ou

d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations sexuelles de la part d'une personne qui se livre à la prostitution, y compris de façon occasionnelle, lorsque cette personne présente une particulière vulnérabilité, apparente ou connue de son auteur, due à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse " ;

- Quant au nouvel article 225-10-1 du code pénal :

59. Considérant que les auteurs des deux saisines reprochent au nouvel article 225-10-1 du code pénal de porter atteinte aux principes de la nécessité et de la légalité des peines ; qu'il méconnaîtrait en outre, selon eux, le principe de la dignité de la personne humaine ;

60. Considérant qu'il est loisible au législateur de prévoir de nouvelles infractions en déterminant les peines qui leur sont applicables ; que, toutefois, il lui incombe d'assurer, ce faisant, la conciliation entre les exigences de l'ordre public et la garantie des droits constitutionnellement protégés ; qu'il lui incombe également, en vertu de l'article 8 de la Déclaration de 1789, de respecter le principe de la légalité des peines et le principe de la nécessité et de la proportionnalité des peines et des sanctions ;

61. Considérant, en premier lieu, que le racolage public est susceptible d'entraîner des troubles pour l'ordre public, notamment pour la tranquillité, la salubrité et la sécurité publiques ; qu'en privant le proxénétisme de sources de profit, la répression du racolage sur la voie publique fait échec au trafic des êtres humains ; que la création par le législateur d'un délit de racolage public ne se heurte dès lors à aucune règle, ni à aucun principe de valeur constitutionnelle ;

62. Considérant, en deuxième lieu, que le principe de légalité des peines n'est pas méconnu par les dispositions critiquées, dès lors que celles-ci définissent en termes clairs et précis le délit de racolage public ;

63. Considérant, enfin, que les peines prévues par le nouvel article 225-10-1 du code pénal ne sont pas manifestement disproportionnées ; qu'il appartiendra cependant à la juridiction compétente de prendre en compte, dans le prononcé de la peine, la circonstance que l'auteur a agi sous la menace ou par contrainte ; que, sous cette réserve, la disposition critiquée n'est pas contraire au principe de la nécessité des peines ;

- Quant au nouvel alinéa ajouté à l'article 225-12-1 du code pénal :

64. Considérant que, selon les sénateurs requérants, cette disposition méconnaîtrait le principe selon lequel nul ne peut être sanctionné que de son propre fait et celui selon lequel la définition des crimes et délits doit comporter un élément intentionnel ;

65. Considérant, d'une part, que le délit n'est constitué que si la vulnérabilité de la personne qui se prostitue est apparente ou connue de l'auteur ; que, d'autre part, cette vulnérabilité est précisément définie par son caractère " particulier " et par le fait qu'elle est due à la maladie, à une déficience physique ou psychique ou à l'état de grossesse ; que, par suite, les deux principes de valeur constitutionnelle invoqués par les sénateurs requérants sont respectés en l'espèce ;

- SUR L'ARTICLE 51 :

66. Considérant que l'article 51 de la loi déferée complète par un 4° l'article 225-10 du code pénal en vue de réprimer le fait, par quiconque, agissant directement ou par personne interposée, " de vendre, de louer ou de tenir à la disposition, de quelque manière que ce soit, d'une ou plusieurs personnes, des véhicules de toute nature en sachant qu'elles s'y livreront à la prostitution " ;

67. Considérant que, contrairement aux affirmations contenues dans les deux saisines, ces dispositions n'interdisent nullement aux

personnes qui se prostituent d'acquérir un véhicule et de l'utiliser ; qu'elles ne portent pas non plus atteinte à la liberté d'entreprendre des vendeurs et loueurs de véhicules, qui trouve sa limite dans le fait de contribuer, en toute connaissance de cause, à des activités illicites ou contraires à l'ordre public ;
 - SUR L'ARTICLE 53 :

68. Considérant que cet article insère les articles 322-4-1 et 322-15-1 dans le code pénal ; que le premier de ces articles dispose que " Le fait de s'installer en réunion, en vue d'y établir une habitation, même temporaire, sur un terrain appartenant soit à une commune qui s'est conformée aux obligations lui incombant en vertu du schéma départemental prévu par l'article 2 de la loi n° 2000-614 du 5 juillet 2000 relative à l'accueil et à l'habitat des gens du voyage ou qui n'est pas inscrite à ce schéma, soit à tout autre propriétaire autre qu'une commune, sans être en mesure de justifier de son autorisation ou de celle du titulaire du droit d'usage du terrain, est puni de six mois d'emprisonnement et de 3 750euros d'amende. - Lorsque l'installation s'est faite au moyen de véhicules automobiles, il peut être procédé à leur saisie, à l'exception des véhicules destinés à l'habitation, en vue de leur confiscation par la juridiction pénale " ; qu'aux termes du nouvel article 322-15-1 du code pénal : " Les personnes physiques coupables de l'infraction prévue à l'article 322-4-1 encourent les peines complémentaires suivantes : - 1° La suspension, pour une durée de trois ans au plus, du permis de conduire ; - 2° La confiscation du ou des véhicules automobiles utilisés pour commettre l'infraction, à l'exception des véhicules destinés à l'habitation " ;

69. Considérant que, selon les députés et sénateurs requérants, les mesures ainsi prévues portent une atteinte disproportionnée aux droits des " gens du voyage " en raison des restrictions qu'elles imposent à leur mode de vie ; qu'il en irait ainsi de la suspension du permis de conduire et de la saisie des véhicules servant à tracter les caravanes ; que les dispositions critiquées méconnaîtraient en outre le principe selon lequel la définition des délits et des peines doit comporter un élément intentionnel, dès lors que certains des occupants du terrain pourraient ne pas être conscients d'user de la propriété d'autrui sans autorisation ;

70. Considérant que la prévention d'atteintes au droit de propriété et à l'ordre public sont nécessaires à la sauvegarde de principes et de droits de valeur constitutionnelle ; qu'il appartient cependant au législateur, en prévoyant la répression de telles atteintes, d'assurer la conciliation entre ces exigences constitutionnelles et l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté d'aller et venir, le respect de la vie privée et l'inviolabilité du domicile ; qu'il lui revient également, compte tenu des objectifs qu'il s'assigne, de fixer, dans le respect des principes constitutionnels, les règles concernant la détermination des crimes et délits, ainsi que des peines qui leur sont applicables ;

71. Considérant, en premier lieu, que le législateur n'a pas entaché d'erreur manifeste la conciliation qu'il lui appartenait d'opérer en l'espèce entre, d'une part, la protection de la propriété et la sauvegarde de l'ordre public et, d'autre part, l'exercice des libertés constitutionnellement protégées ;

72. Considérant, en deuxième lieu, qu'en l'absence de disproportion manifeste entre les infractions et les sanctions concernées, il n'appartient pas au Conseil constitutionnel de substituer son appréciation à celle du législateur ; qu'eu égard à la nature des pratiques en cause, le législateur n'a pas méconnu le principe de nécessité des peines en prévoyant les peines complémentaires de suspension du permis de conduire pendant une durée maximale de trois ans et la confiscation des véhicules automobiles utilisés pour commettre

l'infraction, à l'exception de ceux destinés à l'habitation ;
 73. Considérant, en troisième lieu, que l'occupation du terrain d'autrui rend vraisemblable la volonté de commettre l'infraction ; que la condamnation de l'ensemble des occupants illicites du terrain dans les conditions prévues par la disposition contestée n'est pas contraire à l'article 9 de la Déclaration de 1789 dès lors que s'appliqueront de plein droit, dans le respect des droits de la défense, les principes généraux du droit pénal énoncés aux articles 121-3 et 122-3 du code pénal, qui précisent respectivement qu'" Il n'y a point de délit sans intention de le commettre " et que " N'est pas pénalement responsable la personne qui justifie avoir cru, par une erreur sur le droit qu'elle n'était pas en mesure d'éviter, pouvoir légitimement accomplir l'acte " ;
 74. Considérant, enfin, que la distinction opérée par l'article critiqué entre les communes qui se sont conformées aux obligations que leur impose la loi du 5 juillet 2000 susvisée relative à l'accueil et à l'habitat des gens du voyage et les communes qui ont négligé de le faire repose sur des critères objectifs et rationnels en rapport direct avec le but que s'est assigné le législateur en vue d'accueillir les gens du voyage dans des conditions compatibles avec l'ordre public et les droits des tiers ; que c'est dès lors à tort que les députés requérants soutiennent que l'incrimination critiquée serait contraire au principe d'égalité devant la loi pénale ;
 75. Considérant qu'il résulte de tout ce qui précède que, sous la réserve énoncée au considérant 73, l'article 53 n'est pas contraire à la Constitution ;
 - SUR L'ARTICLE 64 :
 76. Considérant que l'article 64 insère dans le code pénal une section 2 ter intitulée " de l'exploitation de la mendicité " ; que l'exploitation de la mendicité est notamment définie, aux termes du 2° du nouvel article 225-12-5 du code pénal, par le fait " d'en partager les bénéfices " ; que les auteurs des deux recours font valoir que cette disposition définit un délit dépourvu de caractère intentionnel et serait dès lors contraire aux articles 8 et 9 de la Déclaration de 1789 ;
 77. Considérant toutefois que s'appliquera de plein droit à la définition critiquée, dans le respect des droits de la défense, le principe général du droit pénal énoncé à l'article 121-3 du code pénal qui précise qu'" Il n'y a point de délit sans intention de le commettre " ; que, sous cette réserve, la disposition contestée ne méconnaît pas les articles 8 et 9 de la Déclaration de 1789 ;
 - SUR L'ARTICLE 65 :
 78. Considérant que cet article insère dans le code pénal un article 312-12-1 ainsi rédigé : " Le fait, en réunion et de manière agressive, ou sous la menace d'un animal dangereux, de solliciter, sur la voie publique, la remise de fonds, de valeurs ou d'un bien, est puni de six mois d'emprisonnement et de 3 750 euros d'amende " ;
 79. Considérant que, selon les députés et sénateurs requérants, cette disposition permet de réprimer des comportements tombant déjà sous le coup du délit d'extorsion de fonds défini à l'article 312-1 du code pénal ; qu'ils soutiennent qu'une telle " double incrimination " serait contraire au principe de nécessité des peines ;
 80. Considérant que le délit défini à l'article 65 vise, par ses éléments constitutifs, des agissements distincts de ceux mentionnés à l'article 312-1 du code pénal ; que le moyen tiré d'une double incrimination manque dès lors en fait ;
 - SUR L'ARTICLE 75 :

81. Considérant que l'article 75 modifie l'ordonnance du 2 novembre 1945 susvisée relative aux conditions d'entrée et de séjour des étrangers en France ; qu'il ajoute notamment au dernier alinéa de son article 12 une phrase ainsi rédigée : " La carte de séjour temporaire peut être retirée à l'étranger passible de poursuites pénales sur le fondement des articles 225-4-1 à 225-4-4, 225-4-7, 225-5 à 225-11, 225-12-5 à 225-12-7, 311-4 (7°) et 312-12-1 du code pénal " ;
82. Considérant qu'il est fait grief à cette disposition par les députés requérants de placer les étrangers sous un régime arbitraire, ainsi que de porter atteinte à la présomption d'innocence, aux droits de la défense et au droit de chacun à une vie familiale normale ;
83. Considérant qu'aucun principe, non plus qu'aucune règle de valeur constitutionnelle, n'assure aux étrangers des droits de caractère général et absolu de séjour sur le territoire national ; que, dès lors, le législateur peut, sans méconnaître aucun droit ni aucun principe de valeur constitutionnelle, subordonner le maintien ou la délivrance d'un titre temporaire de séjour à l'absence de menace pour l'ordre public ;
84. Considérant qu'eu égard à la nature des infractions visées, qui portent toutes préjudice à l'ordre public, il était loisible au législateur de permettre le retrait de la carte de séjour temporaire des personnes passibles de poursuites de ce chef ; que, pour l'application de la disposition contestée, éclairée par les débats parlementaires, il conviendra cependant d'entendre par " personnes passibles de poursuites " les seuls étrangers ayant commis les faits qui les exposent à l'une des condamnations prévues par les dispositions du code pénal auxquelles renvoie l'article 75 de la loi déferée ;
85. Considérant que, si le principe de la présomption d'innocence ne peut être utilement invoqué en dehors du domaine répressif, ni le principe des droits de la défense utilement invoqué à l'encontre du retrait de la carte de séjour pour des motifs d'ordre public, lequel constitue non une sanction mais une mesure de police, l'intéressé sera mis à même de présenter ses observations sur la mesure de retrait envisagée dans les conditions prévues par la législation de droit commun relative à la procédure administrative ;
86. Considérant, toutefois, qu'il appartiendra à l'autorité compétente, lorsqu'elle envisagera de faire application de la disposition contestée, de prendre en considération le droit de chacun à mener une vie familiale normale ;
87. Considérant qu'il résulte de ce qui précède que, sous les réserves énoncées aux considérants 84, 85 et 86, l'article 75 n'est pas contraire à la Constitution ;
- SUR L'ARTICLE 76 :
88. Considérant qu'aux termes des deux premiers alinéas de l'article 76 de la loi déferée : " Sauf si sa présence constitue une menace à l'ordre public, une autorisation provisoire de séjour peut être délivrée à l'étranger qui dépose plainte contre une personne qu'il accuse d'avoir commis à son encontre les infractions visées aux articles 225-4-1 à 225-4-6 et 225-5 à 225-10 du code pénal ou témoigne dans une procédure pénale concernant une personne poursuivie pour ces mêmes infractions. Cette autorisation provisoire de séjour ouvre droit à l'exercice d'une activité professionnelle. - En cas de condamnation définitive de la personne mise en cause, une carte de résident peut être délivrée à l'étranger ayant déposé plainte ou témoigné " ;
89. Considérant que, selon la saisine sénatoriale, ces dispositions porteraient atteinte à la liberté individuelle des étrangers qui se livrent à la prostitution ;
90. Considérant qu'en dehors de la délivrance de l'autorisation de travail, les dispositions contestées ne créent aucun droit nouveau au

profit des étrangers et ne les soumettent à aucune obligation nouvelle ; qu'elles ne confèrent pas non plus à l'autorité administrative des pouvoirs dont elle ne disposerait pas déjà ; qu'elles sont par suite, et dans cette mesure, dépourvues de caractère normatif et ne sauraient donc être utilement arguées d'inconstitutionnalité ;

91. Considérant que la délivrance d'une autorisation de travail aux étrangers concernés ne porte atteinte ni à leur liberté individuelle ni à aucun autre de leurs droits constitutionnellement garantis ;

- SUR L'ARTICLE 96 :

92. Considérant que le II de l'article 96 introduit les articles 3-1 et 3-2 dans la loi du 12 juillet 1983 susvisée réglementant les activités privées de surveillance, de gardiennage et de transport de fonds ;

93. Considérant qu'aux termes du nouvel article 3-1 de la loi du 12 juillet 1983 : " Les personnes physiques exerçant l'activité mentionnée au 1° de l'article 1er peuvent procéder à l'inspection visuelle des bagages à main et, avec le consentement de leur propriétaire, à leur fouille - Les personnes physiques exerçant l'activité mentionnée au 1° de l'article 1er, spécialement habilitées à cet effet et agréées par le préfet du département ou, à Paris, par le préfet de police dans les conditions prévues par décret en Conseil d'Etat, peuvent, en cas de circonstances particulières liées à l'existence de menaces graves pour la sécurité publique, procéder, avec le consentement exprès des personnes, à des palpations de sécurité. Dans ce cas, la palpation de sécurité doit être faite par une personne de même sexe que la personne qui en fait l'objet. Ces circonstances particulières sont constatées par un arrêté du préfet qui en fixe la durée et détermine les lieux ou catégories de lieux dans lesquels les contrôles peuvent être effectués. Cet arrêté est communiqué au procureur de la République " ;

94. Considérant qu'aux termes du nouvel article 3-2 de ladite loi : " Pour l'accès aux enceintes dans lesquelles est organisée une manifestation sportive, récréative ou culturelle rassemblant plus de 1 500 spectateurs, les personnes physiques exerçant l'activité mentionnée au 1° de l'article 1er, agréées par le préfet dans les conditions prévues par décret en Conseil d'Etat, ainsi que celles, membres du service d'ordre affecté par l'organisateur à la sécurité de la manifestation sportive, récréative ou culturelle en application des dispositions de l'article 23 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, titulaires d'un diplôme d'Etat et agréées par le préfet, peuvent procéder, sous le contrôle d'un officier de police judiciaire et avec le consentement exprès des personnes, à des palpations de sécurité. Dans ce cas, la palpation doit être effectuée par une personne de même sexe que la personne qui en fait l'objet. - Elles peuvent, ainsi que les agents de police municipale affectés sur décision du maire à la sécurité de la manifestation, procéder à l'inspection visuelle des bagages à main et, avec le consentement de leur propriétaire, à leur fouille. - A Paris, les pouvoirs conférés au préfet par le présent article sont exercés par le préfet de police " ;

95. Considérant que les auteurs des deux saisines font grief à ces dispositions de porter atteinte à la liberté individuelle et d'être formulées de façon trop imprécise ;

96. Considérant, ainsi qu'il ressort des termes mêmes des dispositions contestées, qu'en les édictant, le législateur a posé des règles claires et précises ; que, par suite, il n'est pas resté en deçà de sa compétence ;

97. Considérant que le nouvel article 3-1 de la loi du 12 juillet 1983 impose une stricte procédure d'agrément en vue d'habiliter des

personnels de sécurité privés à participer à des opérations de contrôle ; que ces derniers ne peuvent procéder, sans le consentement de l'intéressé, qu'à l'inspection visuelle des bagages à main ; que l'opération dans le cadre de laquelle ils peuvent pratiquer, sauf refus des personnes concernées, des palpations de sécurité ou des fouilles de bagages à main ne peut être ordonnée que par le préfet, en raison de menaces graves pour la sécurité publique et de circonstances particulières, pour un temps et dans des lieux déterminés ; que les modalités ainsi prévues ne portent pas atteinte à la liberté individuelle ; qu'une telle mesure de police administrative, dont la nécessité sera contrôlée par la juridiction administrative, n'est contraire par elle-même à aucun principe, ni à aucune règle de valeur constitutionnelle ;

98. Considérant qu'il en va de même du nouvel article 3-2 de la loi du 12 juillet 1983 ; qu'en effet, l'accès aux enceintes où se déroulent de grandes manifestations sportives, culturelles et récréatives justifie des mesures de surveillance particulières pour protéger la sécurité physique des participants ; qu'aucune des mesures prévues par ledit article ne porte atteinte à la liberté individuelle ;

- SUR L'ARTICLE 113 :

99. Considérant que cet article insère dans le code pénal un article 433-5-1 ainsi rédigé : " Le fait, au cours d'une manifestation organisée ou réglementée par les autorités publiques, d'outrager publiquement l'hymne national ou le drapeau tricolore est puni de 7 500 euros d'amende. - Lorsqu'il est commis en réunion, cet outrage est puni de six mois d'emprisonnement et de 7 500 euros d'amende " ;

100. Considérant que les députés et sénateurs requérants estiment que ces dispositions portent " une atteinte grave à la liberté d'expression, de conscience et d'opinion " ; qu'elles sont en outre contraires " au principe de légalité des délits et des peines et au principe de nécessité des sanctions " ;

101. Considérant, d'une part, que l'article 10 de la Déclaration de 1789 dispose que " Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi " ; qu'en vertu de l'article 11 de la Déclaration : " La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre à l'abus de cette liberté dans les cas déterminés par la loi " ;

102. Considérant, d'autre part, qu'aux termes du deuxième alinéa de l'article 2 de la Constitution " L'emblème national est le drapeau tricolore, bleu, blanc, rouge " ; qu'à ceux de son troisième alinéa : " L'hymne national est La Marseillaise " ;

103. Considérant, enfin, qu'il est loisible au législateur de prévoir de nouvelles infractions en déterminant les peines qui leur sont applicables ; que, toutefois, il lui incombe d'assurer, ce faisant, la conciliation des exigences de l'ordre public et la garantie des libertés constitutionnellement protégées ;

104. Considérant que sont exclus du champ d'application de l'article critiqué les oeuvres de l'esprit, les propos tenus dans un cercle privé, ainsi que les actes accomplis lors de manifestations non organisées par les autorités publiques ou non réglementés par elles ; que l'expression " manifestations réglementées par les autorités publiques ", éclairée par les travaux parlementaires, doit s'entendre des manifestations publiques à caractère sportif, récréatif ou culturel se déroulant dans des enceintes soumises par les lois et règlements à des règles d'hygiène et de sécurité en raison du nombre de personnes qu'elles accueillent ;

105. Considérant qu'en instituant un tel délit, le législateur a effectué la conciliation qu'il lui appartenait d'assurer entre les exigences constitutionnelles rappelées ci-dessus ; que la peine qu'il a fixée ne revêt pas de caractère manifestement disproportionné par rapport à

l'infraction ;

106. Considérant qu'il résulte de ce qui précède que, sous la réserve d'interprétation énoncée au considérant 104, l'article 113 de la loi déférée n'est pas contraire à la Constitution ;

- SUR LES ARTICLES 122 ET 123 :

107. Considérant que les articles 122 et 123 de la loi déférée appliquent respectivement en Nouvelle-Calédonie et en Polynésie française des dispositions analogues à celles de son article 3 ; que les députés requérants leur adressent les mêmes reproches ; que, pour des motifs identiques à ceux exposés à propos de l'article 3, les moyens ainsi invoqués doivent être écartés ;

- SUR LES ARTICLES 141 ET 142 :

108. Considérant que les articles 141 et 142 pérennisent en Guyane et dans la commune de Saint-Martin en Guadeloupe les dispositions dérogatoires rendues applicables pour cinq ans dans les départements d'outre-mer par la loi du 11 mai 1998 susvisée ; qu'en vertu de ces dispositions, les refus de délivrance de titre de séjour à certains étrangers ne sont pas soumis pour avis à la commission du titre de séjour prévue par l'article 12 quater de l'ordonnance du 2 novembre 1945 et le recours dirigé contre un arrêté de reconduite d'un étranger à la frontière ne revêt pas de caractère suspensif ;

109. Considérant que les députés requérants soutiennent qu'en pérennisant un tel régime, les articles 141 et 142 méconnaissent " des droits et garanties constitutionnellement protégés, tels que les droits de la défense " et vont au-delà des adaptations au régime législatif des départements d'outre-mer autorisées par l'article 73 de la Constitution ;

110. Considérant que le législateur a pu, pour prendre en compte la situation particulière et les difficultés durables du département de la Guyane et, dans le département de la Guadeloupe, de la commune de Saint-Martin, en matière de circulation internationale des personnes, y maintenir le régime dérogatoire institué par les articles 12 quater et 40 de l'ordonnance du 2 novembre 1945 susvisée, sans rompre l'équilibre que le respect de la Constitution impose d'assurer entre les nécessités de l'ordre public et la sauvegarde des droits et libertés constitutionnellement garantis ; que les intéressés conserveront un droit de recours juridictionnel contre les mesures de police administrative ; qu'ils auront notamment la faculté de saisir le juge des référés administratifs ; que le législateur n'a pas non plus porté atteinte au principe constitutionnel d'égalité compte tenu de cette situation particulière, laquelle est en relation directe avec l'objectif qu'il s'est fixé de renforcer la lutte contre l'immigration clandestine ; que les adaptations ainsi prévues ne sont pas contraires à l'article 73 de la Constitution ;

111. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune question de conformité à la Constitution,

Décide :

Article premier :

Ne sont pas contraires à la Constitution, sous les réserves énoncées aux considérants 26, 34, 35, 38, 43, 57, 63, 73, 77, 84, 85, 86 et 104, les dispositions de la loi pour la sécurité intérieure critiquées par l'une ou l'autre saisine.

Article
La présente décision sera publiée au ² Journal officiel de la République française :

Délibéré par le Conseil constitutionnel dans sa séance du 13 mars 2003, où siégeaient : MM. Yves GUÉNA, Président, Michel AMELLER, Jean-Claude COLLIARD, Olivier DUTHEILLET de LAMOTHE, Pierre JOXE, Pierre MAZEAUD, Mmes Monique PELLETIER, Dominique SCHNAPPER et Simone VEIL.

Publication Journal officiel du 19 mars 2003, p. 4789