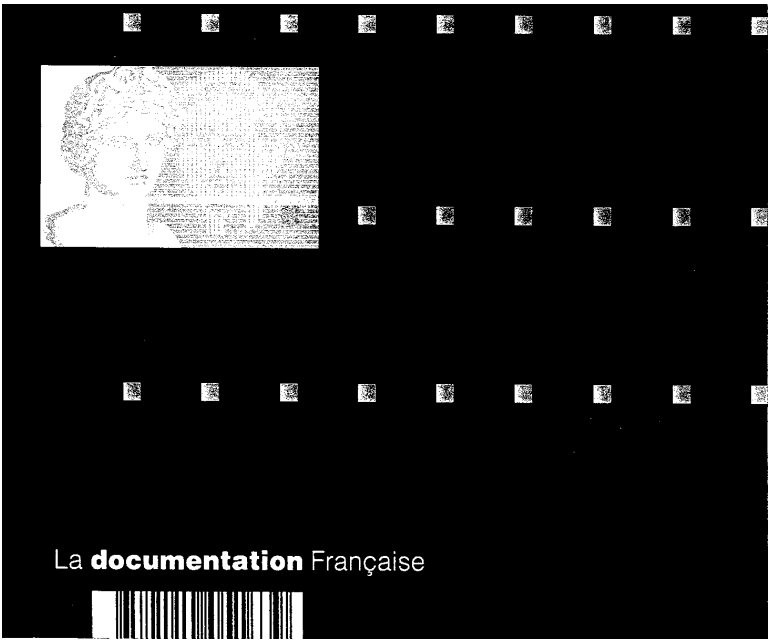
22e rapport d'activité 2001

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Édition 2002


La **documentation** Française

COMMISSION
NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

22e rapport d'activité 2001

prévu par l'article 23 de la loi du 6 janvier 1978

ISBN 2-11-005163-9

Sommaire

Avant-propos

Les premières années de l'Internet commercial et « grand public » ont été marquées par de vifs débats. Le réseau international était-il « hors-loi » ? Fallait-il légiférer ou s'en remettre à l'autorégulation. S'agissant tout particulièrement de la collecte et du traitement des données personnelles et des traces invisibles attachées à nos connexions, nos droits et principes pouvaient-ils s'appliquer avec quelque effectivité aux multiples usages de l'Internet ? En un mot, fallait-il, à l'heure de la « mondialisation numérique », remettre en cause le fondement de législations forgées en Europe il y a plus de vingt ans ?

Le temps paraît venu de la maturité.

En témoigne d'abord l'universalisation des principes de protection des données personnelles, tels que nous les connaissons en Europe. Avant de conclure les accords dits du *safe harbor* avec la Commission européenne, garantissant ainsi un niveau de protection adéquat aux données personnelles communiquées aux entreprises adhérentes américaines, les États-Unis avaient adopté une loi destinée à protéger les mineurs à l'égard de la collecte et du traitement de leurs données personnelles (la loi COPPA). Dans le même temps diverses décisions de justice américaines ont consacré une place, jusqu'alors inédite, à la préoccupation des données personnelles. Le présent rapport annuel de la CNIL en rend compte, comme des initiatives prises par le Canada ou l'Australie pour étendre le champ de leur loi « informatique et libertés » aux fichiers des entreprises privées tandis que neuf pays d'Europe centrale et orientale se sont dotés, en la matière, de législations comparables à celles des États membres de l'Union européenne.

Le temps de la maturité, c'est aussi, pour la CNIL, le temps de l'action. Qu'il s'agisse du sort du fichier des abonnés de Canal+ lors de la fusion Vivendi Universal, de la cybersurveillance sur les lieux de travail, de la diffusion sur Internet de décisions de justice sous leur forme nominative, de la constitution d'un système national d'informations sur les dépenses de santé rassemblant des données particulièrement sensibles, de la crainte d'un risque discriminatoire lié au traitement de l'information relative aux demandeurs de logements sociaux, de l'attention particulière qu'appelle la collecte de données auprès des mineurs, la Commission s'est efforcée, au travers de recommandations particulières ou de rapports d'ensemble rendus publics, de tracer des lignes et d'inviter à de nouvelles pratiques. Le chapitre de ce rapport consacré aux interventions de la CNIL sur ces sujets devrait contribuer à une meilleure connaissance des éléments de doctrine de la Commission et des orientations ainsi dégagées.

Le temps de la maturité doit être également celui des débats dans lesquels, au-delà de l'attrait de la nouveauté technologique, sinon de l'exaltation des concepts, les enjeux soient posés aussi clairement qu'il est possible, et le soient pour le plus grand nombre. La Commission s'y est efforcée en abordant dans un chapitre

consacré aux « débats en cours », la question de « l'identité numérique », laquelle doit d'abord être perçue comme un marché qui s'ouvre sous l'effet conjugué de la standardisation des protocoles et de la convergence, le défi de « l'administration électronique » dont un projet du ministère de l'Economie, des Finances et de l'Industrie préfigure, sous le programme « Copernic », quelques grandes tendances, mais aussi l'essor de la biométrie que les progrès technologiques et la baisse des coûts font sortir du champ policier auquel elle était jusqu'alors principalement cantonnée. Les développements consacrés aux techniques de reconnaissance des visages donnent la dimension des problèmes éthiques nouveaux auxquels nous pourrions être confrontés. Dans un tout autre domaine, la multiplication des fichiers communs de lutte contre la fraude, notamment au crédit, appelle sans doute à une intervention législative, à défaut de laquelle le développement de véritables « listes noires » propices à de nouvelles formes d'exclusion sociale serait à redouter.

D'importantes modifications législatives intervenues ces derniers mois paraissent également attester ce temps de la maturité dans des domaines aussi sensibles que le droit d'accès des malades à leur dossier médical, la consultation des fichiers de police judiciaire dans le cadre de certaines enquêtes administratives de moralité des candidats à l'exercice de missions de sécurité ou de défense, l'extension du fichier des empreintes génétiques à des fins criminelles ou la délicate question de la conservation des données de connexion à Internet. Les avis de la CNIL, lorsqu'ils ont été sollicités sur ces projets, ont quelquefois été suivis ; ils ont toujours pesé.

L'essentiel, surtout après les événements si dramatiques du 11 septembre 2001, n'est-il pas que l'Europe, et la France parmi les premières, ait donné l'exemple en instituant une autorité indépendante chargée de veiller aux incidences multiples des nouvelles technologies sur le respect de notre vie privée mais aussi sur les libertés individuelles ou publiques, comme le proclame l'article premier de la loi du 6 janvier 1978 ? Non pas qu'il s'agisse pour les États de déléguer le pouvoir de décision que leur confère la légitimité démocratique. Pas davantage qu'il convienne de préférer l'expertise au débat public. Mais bien parce qu'il s'agit, dans des champs de plus en plus divers, de positionner le curseur au plus juste de l'équilibre entre « sécurité » et « liberté ». À cet égard nous devons nous réjouir que des États, de plus en plus nombreux, s'imposent de recueillir l'avis ou le sentiment d'une autorité moins directement soumise aux contingences du temps ou de l'opinion avant d'arrêter des décisions qu'il leur appartient de prendre.

Tels étaient en tout cas les enseignements de la 23e conférence internationale des commissaires à la protection des données que la CNIL a accueilli à Paris du 24 au 26 septembre 2001 et qui, au moment où résonnait l'écho du monde, a témoigné de cette commune conviction.

Il reste à souhaiter que ce temps de la maturité permette, maintenant sans tarder, que soit définitivement adoptée une loi « informatique et libertés » actualisée et rénovée, transposant la directive européenne du 24 octobre 1995 et permettant à la Commission d'exercer les missions qui lui sont confiées avec la vigueur nouvelle qu'appellent les enjeux de notre temps.

Michel GENTOT

Chapitre 1

L'ANNÉE 2001 ET LA PROTECTION DES DONNÉES

I. LA CNIL EN CHIFFRES

A. Les saisines

Les articles 6, 21,22 et 39 de la loi du 6 janvier 1978 confient à la CNIL la mission d'informer les personnes de leurs droits et obligations, de tenir à leur disposition le registre des traitements déclarés (« fichier des fichiers »), de recevoir les réclamations, pétitions et plaintes, ainsi que d'exercer, à la demande des requérants, le droit d'accès aux fichiers intéressant la sécurité publique et la sûreté de l'État.

Nature des saisines	1995	1996	1997	1998	1999	2000	2001	Variation 2000/2001
Demandes de droit d'accès indirect	243	320	385	401	671	817	**836**	+ 2,3 %
Plaintes	1 636	2 028	2 348	2 671	3 508	3 399	**3 574**	+ 5,1 %
Demandes de conseil	985	1 008	821	1 115	1 061	1 049	**973**	- 7,2 %
Demandes de radiation des fichiers commerciaux	263	277	263	204	186	144	**94**	- 34,7 %
Demandes d'extraits du fichier des fichiers	122	170	155	154	133	208	**252**	+ 21,1 %
Total	**3 249**	**3 803**	**3 972**	**4 545**	**5 559**	**5617**	**5 729**	+ 2,0 %

Au cours de l'année 2001, la CNIL a enregistré **une augmentation :**

— des demandes d'exercice du droit d'accès indirect aux fichiers de police et de sécurité de + 2,3 %, et ce malgré la très forte croissance enregistrée les deux années précédentes (+67 % en 1999 et +21 % en 2000) ;

— des plaintes de + 5,1 %, alors que leur nombre annuel a plus que doublé depuis 1995 ;

— des demandes d'extrait du « fichier des fichiers » de + 21,1 %, ce qui montre la volonté croissante des citoyens de connaître le sort des données les concernant, notamment en exerçant leurs droits d'accès ou de rectification.

Par ailleurs, la nette baisse des demandes de radiation des fichiers commerciaux (-34,7 %) est certainement, pour partie, la conséquence de nombreuses années d'actions de sensibilisation à la loi « informatique et libertés » menées dans le secteur du marketing.

De la même façon, la baisse de 7 % constatée sur les demandes de conseil est vraisemblablement la conséquence d'une meilleure information des déclarants grâce à la diffusion de plusieurs guides pratiques (santé, collectivités locales, Internet...), et en particulier leur mise en ligne sur le site web de la CNIL (www.cnil.fr).

À cet égard, la fréquentation du site de la CNIL depuis sa création en 1998 a connu une progression exponentielle : le nombre de pages vues en 2001 atteint 13 millions contre 3,6 millions en 1999 et le nombre de visiteurs a été de 900 000 en 2001 contre 380 000 en 1999.

À titre de rappel, la CNIL a reçu depuis 1978 plus de 11 500 demandes de conseil et plus de 36 200 plaintes (au 31 décembre 2001).

En 2001, les secteurs d'activité qui ont suscité le nombre le plus important de demandes de conseil sont, par ordre décroissant :

— le travail ;
— la santé ;
— l'immobilier ;
— la fiscalité.

Les demandes de conseil portent le plus fréquemment sur les formalités préalables à la mise en oeuvre des fichiers.

Les secteurs d'activité qui ont suscité en 2001 le nombre le plus important de plaintes sont, par ordre décroissant :

— la prospection commerciale ;
— la banque ;
— le travail ;
— les télécommunications.

L'objet le plus fréquent des plaintes concerne l'exercice des droits, et tout particulièrement du droit d'opposition à figurer dans un traitement ou à faire l'objet de prospection commerciale (795 plaintes), mais également l'exercice du droit d'accès aux données (206 plaintes).

L'instruction des plaintes peut conduire la CNIL à délivrer un avertissement ou à dénoncer des faits au parquet, conformément à l'article 21 alinéa 4 de la loi du 6 janvier 1978.

En 2001, la CNIL n'a délivré aucun avertissement, ce qui maintient à quarante-sept le nombre d'avertissements émis depuis 1978. En revanche, la CNIL a transmis à la justice une affaire de divulgation sur Internet d'informations sensibles. Cela porte à dix-huit le nombre de dénonciations au parquet effectuées depuis 1978 (*cf. infra* chapitre 2, délibération n° 01-042 du 10 juillet 2001).

B. Le droit d'accès indirect

En application des articles 39 et 45 de la loi du 6 janvier 1978, toute personne a le droit de demander que des vérifications soient entreprises par la CNIL sur les renseignements la concernant pouvant figurer dans des traitements automatisés et des fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique. Aucun fichier de cette nature n'échappe à de telles vérifications. Les investigations sont effectuées par les membres de la Commission appartenant ou ayant appartenu au Conseil d'État, à la Cour de Cassation ou à la Cour des comptes : c'est ce dispositif qui est communément appelé « droit d'accès indirect ».

Depuis 1978, la CNIL a reçu **6 259 demandes de droit d'accès indirect** qui ont donné lieu à plus de **10 000 investigations.** La progression du nombre de requêtes constatée depuis 1996 se poursuit. Ainsi, 836 demandes ont été reçues en 2001, ce qui a conduit la CNIL à entreprendre plus de 1 400 vérifications, une même requête concernant souvent plusieurs traitements ou fichiers.

ÉVOLUTION DES DEMANDES DE DROIT D'ACCÈS INDIRECT DEPUIS 1995

	1995	1996	1997	1998	1999	2000	**2001**
Requêtes	243	320	385	401	671	817	**836**
Évolution		+ 32 %	+ 20 %	+ 4%	+ 67 %	+ 22 %	**+ 2,3 %**

À titre d'exemple, les requérants saisissent la CNIL :

— à la suite d'un refus d'embauche ;
— à la suite d'une enquête d'habilitation défavorable ;
— à l'occasion d'une candidature à un emploi du secteur public ;
— à la suite d'un refus de délivrance de visa ou de titre de séjour du fait de l'inscription dans le système d'information Schengen ;
— à la suite d'une interpellation par les services de police ou de gendarmerie ;
— à la suite d'articles de presse sur les fichiers des Renseignements généraux et de police judiciaire ou d'informations diffusées sur des sites Internet décrivant les modalités de droit d'accès aux fichiers de police.

Au cours de l'année 2001, 1 411 vérifications ont été effectuées, dont 90 % ont été opérées dans les fichiers du ministère de l'Intérieur.

Ministère de l'Intérieur	**1 278**
— Renseignements généraux (RG)	576
— Police judiciaire (PJ)	199
— Police urbaine (PU)	180
— Direction de la surveillance du territoire (DST)	85
— Système d'information Schengen (SIS)	232
— Direction de la sûreté et de la protection du secret (DSPS)	6
Ministère de la Défense	**131**
— Gendarmerie nationale (GEND)	67
— Direction de la protection de la sécurité de la défense (DPSD)	32
— Direction générale de la sécurité extérieure (DGSE)	32
Ministère des Finances	
— Fichier nat. informatisé de documentation de la Direction générale des douanes et droits indirect (FNID)	**2**
— Fichier TRACFIN (action contre les circuits financiers clandestins)	**1**
	1
Total	**1 411**

Le résultat des investigations menées en 2001, qui à l'exclusion de celles relatives aux Renseignements généraux (576) et au système d'information Schengen (232) sont au nombre de 603, est le suivant :

Services	PJ	PU	DST	DSPS	GEND	DPSD	DGSE	FNID	TRACFIN	**Total**	% du total
Pas de fiche	37	121	72	4	20	23	30	1	1	**309**	51,2%
Fiche sans suppression d'informations	122	56	12	2	44	9				**245**	40,6%
Suppression totale ou partielle d'informations	18	3	1		2		1			**25**	4,2 %
Mise à jour de la fiche	22	–	–	–	1	–	1			**24**	4,0 %
Total	**199**	**180**	**85**	**6**	**67**	**32**	**32**	**1**	**1**	**603**	100,0%

Les investigations menées dans les fichiers de police judiciaire et en particulier dans le système de traitement des infractions constatées (STIC) ont conduit la CNIL à faire procéder dans **25** % **des cas à des mises à jour, ou même à la suppression de signalements erronés ou manifestement non justifiés** (quarante saisines sur les 162 requérants fichés à la police judiciaire).

Par exemple, une personne signalée par erreur comme auteur d'un meurtre, une jeune fille dont la fugue portée à la connaissance de la police par les parents avait conduit à son inscription dans le STIC ou encore un enfant de 7 ans signalé dans le STIC pour avoir jeté des cailloux sur un véhicule...

LES FICHIERS DES RENSEIGNEMENTS GENERAUX

Le décret du 14 octobre 1991 a fixé les modalités particulières d'exercice du droit d'accès aux fichiers des Renseignements généraux. Les membres désignés par la CNIL pour mener ces investigations peuvent, en accord avec le ministre de l'Intérieur, constater que la communication de certaines informations ne met pas en cause la sûreté de l'État, la défense et la sécurité publique et qu'elles peuvent dès lors être communiquées au requérant.

En pratique, trois situations peuvent se présenter :

1) Les Renseignements généraux ne détiennent aucune information nomina tive concernant un requérant, la CNIL en informe ce dernier, en accord avec le ministre de l'Intérieur.

2) Les Renseignements généraux détiennent des informations nominatives concernant un requérant ; les informations qui ne mettent pas en cause la sûreté de l'Etat, la défense et la sécurité publique lui sont communiquées, en accord avec le ministre de l'Intérieur. Dans l'hypothèse d'une communication totale ou partielle d'un dossier, le requérant a la possibilité de rédiger une note d'observation que la Com mission transmet au ministre de l'Intérieur et qui est insérée dans le dossier détenu par les services des RG.

3) Si la communication de tout ou partie des informations peut nuire à la sûreté de l'État, la défense et la sécurité publique, le magistrat de la CNIL procède à l'examen du dossier et s'il y a lieu exerce le droit de rectification ou d'effacement des données inexactes ou des données dont la collecte est interdite par la loi. Le prési dent de la CNIL adresse ensuite au requérant une lettre lui indiquant qu'il a été procé dé aux vérifications conformément aux termes de l'article 39 de la loi du 6 janvier 1978. Cette lettre mentionne que la procédure administrative est close et indique les voies et délais de recours contentieux qui sont ouverts au requérant.

Il convient de préciser que les recherches portent tout à la fois sur le fichier informatique d'indexation, sur le dossier individuel, sur lés extraits de dossiers collectifs contenant des données nominatives sur les demandeurs, ainsi que sur les dossiers conservés dans les sections spécialisées de la Direction centrale des Renseignements généraux. Par ailleurs, lorsqu'un document de synthèse citant des personnes physiques est établi par les services des Renseignements généraux, une mention de ce document est faite dans le registre d'indexation des personnes physiques et si possible dans les dossiers individuels des personnes concernées.

BILAN DES 576 INVESTIGATIONS MENEES EN 2001 DANS LES FICHIERS DES RENSEIGNEMENTS GÉNÉRAUX

	Investigations RG 2001	% du total des vérifications effectuées aux RG
Requérants non fichés aux RG	415	**72%**
Requérants fichés aux RG	161	**28%**
Total	**576**	**100%**

Sur 161 requérants fichés, les dossiers ont été communiqués dans les proportions suivantes :

	Requérants fichés aux RG	% sur le nombre de requérants fichés
Dossiers jugés non communicables	35	22%
Communication refusée par le ministre de l'Intérieur	0	
Communication acceptée par le ministre de l'Intérieur — Communication totale — Communication partielle	126 126	78%
Total	**161**	**100%**

De même que les années précédentes, le ministre de l'Intérieur n'a refusé aucune des propositions de communication de dossiers faites par les membres de la CNIL

La procédure de communication des dossiers, initialement fixée par un protocole du 12 février 1992 arrêté avec le ministre de l'Intérieur, a fait l'objet d'une circulaire complémentaire du 2 juin 1993. Depuis cette date, la consultation des pièces communicables du dossier s'effectue au siège de la CNIL lorsque les requérants sont domiciliés dans la région Ile-de-France ou lorsque, domiciliés dans une autre région, ils font l'objet d'une fiche dans les services des Renseignements généraux de la préfecture de police de Paris. Dans tous les autres cas, la communication est organisée au siège de la préfecture du département dans lequel est domicilié le requérant.

Sur les 126 communications intervenues en 2001, cinquante-sept ont eu lieu au siège de la CNIL et soixante-neuf ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé. À la suite de celles-ci, quatre requérants ont rédigé une note d'observation qui a été, conformément aux prescriptions du décret, insérée dans le dossier des Renseignements généraux les concernant.

Par ailleurs il a été procédé à :
- la suppression totale de quatre dossiers ;
- la suppression partielle de deux dossiers ;
- la mise à jour d'informations dans deux dossiers.

EVOLUTION DES INVESTIGATIONS AUPRÈS DES RENSEIGNEMENTS GÉNÉRAUX DEPUIS 1993

Année	1993	1994	1995	1996	1997	1998	1999	2000	**2001**	**Totaux**
Nombre de demandes traitées	320	273	197	252	352	282	270	365	**576**	2 **887**
Requérants non fichés aux RG (% du total des vérifications)	177 *55%*	164 60%	113 57%	145 58%	213 60%	169 60%	173 64%	261 71 %	**415 72%**	1 **830**
Requérants fichés aux RG (% du total des vérifications)	143 45%	109 40%	84 43%	107 42%	139 40%	113 40%	97 46%	104 29%	**161 28%**	1 **057**
Dossiers jugés non communicables (% sur le nombre de requérants fichés)	50 35%	44 40%	25 30%	33 31 %	*57* 41 %	23 20%	15 15,5 %	18 17%	**35 22%**	**300**
Demandes de communication acceptées (% sur le nombre de requérants fichés) dont :	93 65%	65 60%	59 70%	74 69%	82 59%	90 80%	82 84,5 %	86 83%	**126 78%**	**757**
— communication totale — communication partielle	*75* 18	27 38	44 15	63 11	*75* *7*	84 6	79 3	85 1	**126** **-**	

Il est à observer que depuis neuf ans, le ministre de l'Intérieur ne s'est opposé à aucune des demandes de communication de dossiers présentées par un membre de la CNIL

LE SYSTEME D'INFORMATION SCHENGEN

Depuis l'entrée en vigueur du décret n° 95-577 du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS, aux termes de l'article 6 de ce décret et de l'article 109 et 114 de la convention Schengen, la CNIL a reçu 1 194 demandes de droit d'accès aux fichiers du système d'information Schengen, dont 297 pour 2001. L'évolution du nombre de demandes de droit d'accès au N-SIS par année est la suivante :

Année	1995	1996	1997	1998	1999	2000	2001	**Total**
Nombre	22	20	21	78	359	397	297	**1 194**

Parmi les 1 194 demandes de droit d'accès indirect au système d'information Schengen, 571 requérants étaient signalés.

Ces 571 signalements proviennent par ordre décroissant des pays suivants :

Pays signalant	Nombre de signalements	
Allemagne	290	51,0%
France	202	35,0 %
Italie	51	9,0 %
Espagne	13	2,0 %
Grèce	6	1,0 %
Pays-Bas	5	1,0 %
Belgique	2	0,5 %
Autriche	2	0,5 %
Total	**571**	100,0%

À la suite de l'intervention de la CNIL, 266 signalements ont été supprimés du N-SIS (46,6 %), dont 211 par l'Allemagne, 38 par la France, 9 par l'Italie, 4 par l'Espagne, 3 par les Pays-Bas, 1 par la Belgique.

Dans le cas où aucun signalement n'est enregistré dans le système d'information Schengen, alors même qu'il y a eu un refus de visa, la CNIL poursuit ses investigations en saisissant le ministère des Affaires étrangères afin de connaître le motif du refus, et notamment l'inscription éventuelle du requérant dans un fichier d'attention. Ces fichiers, gérés par le ministère des Affaires étrangères et en particulier par les postes consulaires, sont désormais intégrés dans le nouveau système informatique de délivrance des visas (RMV2), créé par un arrêté du 22 août 2001 pris après avis favorable de la CNIL (*cf.* délibération n° 019-01 du 15 mai 2001 en annexe 5).

Aux termes de l'article 6 de cet arrêté, le droit d'accès aux informations contenues dans le RMV2 est mixte. Ainsi, les informations enregistrées lors de la demande de visa font l'objet d'un accès direct, qui peut être exercé auprès du consulat ou de l'ambassade où la demande a été déposée. En revanche, les informations figurant dans les fichiers d'attention (fichier central comme fichiers locaux), susceptibles de porter atteinte à la sûreté de l'État, la défense et la sécurité publique, font l'objet d'un droit d'accès indirect.

Lors de l'instruction de la demande d'avis concernant cette nouvelle application, le ministère des Affaires étrangères s'est engagé à prendre toutes mesures de nature à faciliter l'exercice de ce droit et à permettre aux commissaires en charge du droit d'accès indirect de vérifier le contenu de la fiche d'attention. Il a ainsi été convenu que le fichier central d'attention pourra être directement consulté par les commissaires en charge du droit d'accès indirect dans les locaux du ministère des Affaires étrangères.

S'agissant des fichiers locaux d'attention, le ministère des Affaires étrangères donnera instruction au poste consulaire concerné de transmettre à Paris les éléments figurant dans le fichier au nom de la personne qui demande à exercer son droit d'accès, de telle sorte que les commissaires de la CNIL puissent vérifier ces données.

C. Les avis préalables à la mise en œuvre des traitements

Au 31 décembre 2001, le nombre de traitements enregistrés par la CNIL depuis 1978 était de 803 765, dont 67,50 % déclarés selon une procédure simplifiée.

	1978-2001	% du total des formalités
Déclarations simplifiées	566 582	67,50 %
Demandes d'avis	45 230	5,39 %
Déclarations ordinaires	190 509	22,70 %
Demandes d'autorisation (chapitre V^{bis} — depuis 1997)	1 304	0,15%
Demandes d'autorisation (chapitre V^{ter} — depuis 1999)	140	0,01 %
Total des traitements enregistrés	**803 765**	—
Déclarations de modification	35 706	4,25 %
Total des formalités préalables	**839 471**	100,00 %

	1997	1998	1999	2000	**2001**	Variation 2000 /2001
Déclarations simplifiées	53 953	50 735	43 571	33 657	**29 755**	- 11,6 %
Demandes d'avis	2 724	3 002	3 538	3 577	**3 868**	+ 8,1 %
Déclarations ordinaires	10 326	11 333	12 200	15 249	**16 119**	+ 5,7 %
Demandes d'autorisation (chapitre V^{bis} — depuis 1997)	133	244	352	287	**288**	+ 0,3 %
Demandes d'autorisation (chapitre V^{ter} — depuis 1999)			8	73	**59**	-19,1 %
Déclarations de modification	2 639	2 358	3 454	2 607	**3 061**	+ 17,4%
Totaux	**69 775**	**67 672**	**63 123**	**55 450**	**53 150**	- **4,1** %

Pour la période du 1er janvier au 31 décembre 2001, la CNIL a enregistré **53 150 nouveaux dossiers de formalités préalables,** dont 3 061 concernent des déclarations de modification de traitements déjà enregistrés. Comme les années passées, les déclarations ordinaires émanant du secteur privé (+5,70 %) et les demandes d'avis du secteur public (+8,13 %) continuent de croître.

Le nombre de sites Internet déclarés progresse considérablement atteignant 7 389 déclarations pour 2001, ce qui constitue une augmentation de 20,85 % par rapport à 2000.

Ce sont en tout 17 262 sites Internet qui étaient recensés à la CNIL au 31 décembre 2001. La liste des sites déclarés à la Commission est accessible directement à partir de son site (www.cnil.fr) dans la rubrique « Sites déclarés ».

	1997	1998	1999	2000	**2001**	**Total**
Déclarations sites Internet	267	930	2 562	6 114[1]	**7 389**	**17 262**

La CNIL a multiplié les initiatives visant à sensibiliser les personnes, responsables de sites ou simples internautes, aux questions de protection des données personnelles. Ainsi, après avoir dévoilé à l'ouverture de son site comment chacun est pisté sur la toile. (« Vos traces sur Internet »), et diffusé un guide pratique « Je monte un site Internet », la Commission a élaboré un rapport d'ensemble sur le publipostage électronique (1999), procédé à une étude d'évaluation de cent sites de commerce électronique (2000) et de soixante sites de santé (2001), avant d'ouvrir à une large consultation publique d'une part, un rapport sur la cybersurveillance des salariés (2001) et d'autre part, un rapport sur « Internet et les mineurs » (2001). Dans le prolongement, la CNIL a mené en 2002 une importante opération de pédagogie en ce qui concerne l'utilisation d'Internet par les enfants *(cf. infra* chapitre 2, VI).

D. Les auditions et contrôles

Dans le cadre de ses missions d'information et de concertation, la CNIL effectue chaque année de nombreuses visites sur place auprès d'entreprises, d'administrations, de collectivités locales, de centres universitaires ou de recherche et procède le cas échéant à des auditions. À ces missions d'information et de concertation, s'ajoutent des missions de contrôle ou de vérification sur place, au titre du contrôle a *posteriori* du fonctionnement des fichiers de données personnelles.

En 2001, la CNIL a procédé à une trentaine de contrôles sur place et à deux auditions en séance plénière.

S'agissant des procédures de contrôles, la CNIL a, en particulier avant d'adopter une recommandation relative aux fichiers de gestion du patrimoine immobilier à caractère social, fichiers qui ont suscité de nombreuses saisines ou plaintes

[1] Dont les déclarations effectuées en ligne à compter du 1er octobre 2000.

auprès de la Commission, effectué plusieurs missions de contrôle auprès d'organismes bailleurs (cf. *infra* chapitre 2, II).

Par ailleurs, la CNIL a procédé à l'audition :

— le 28 juin 2001, du directeur général des impôts et du directeur général de la comptabilité publique, afin que lui soit présenté le programme COPERNIC de refonte du système d'information des administrations fiscales *[cf. infra* chapitre 3, II) ;

— le 9 octobre 2001, du directeur de la Sécurité sociale au ministère de l'Emploi et de la Solidarité, du directeur des exploitations, de la politique sociale et de l'emploi au ministère de l'Agriculture et de la Pêche, des directeurs de la Caisse nationale d'assurance maladie des travailleurs salariés, de la Caisse d'assurance maladie des travailleurs non salariés et non agricoles (CANAM) et de la Mutualité sociale agri cole, à propos de la constitution d'un système national interrégimes de l'assurance maladie *[cf. infra* chapitre 2, IV).

II. LES INTERVENTIONS LEGISLATIVES

A. Libertés publiques : la loi sur la sécurité quotidienne

La loi du 15 novembre 2001 relative à la sécurité quotidienne touche par nature, comme toute loi de police, à la matière des libertés publiques. La CNIL ne tient pas de la loi du 6 janvier 1978 compétence sur l'ensemble des sujets abordés par ce texte, quelle que soit leur importance pour notre sécurité ou nos libertés, ou dans les débats qu'ils ont pu susciter dans l'opinion. En revanche, plusieurs dispositions de cette loi concernent directement des fichiers de données à caractère personnel et les principales d'entre elles méritent, à ce titre, d'être recensées dans le présent rapport.

1 — LA CREATION D'UN FICHIER NATIONAL AUTOMATISE NOMINATIF DES PERSONNES QUI SONT INTERDITES D'ACQUISITION ET DE DÉTENTION D'ARMES

L'article 8 de la loi qui pose le principe de la création d'un tel fichier, dont certains événements récents témoignent de l'utilité et de la nécessité, renvoie à un décret en Conseil d'État, pris après avis de la CNIL, le soin de préciser la nature des informations enregistrées, la durée de leur conservation ainsi que les autorités et les personnes pouvant y avoir accès. À la date de rédaction du présent rapport, la Commission n'a pas été saisie de ce projet de décret.

La tuerie qui a endeuillé le conseil municipal de Nanterre a suscité diverses interrogations sur la coordination des services de l'Etat chargés de délivrer les ports d'armes avec d'autres services éventuellement concernés, s'agissant tout particulièrement de la connaissance de l'état psychologique ou mental du demandeur. Il a pu être, ici ou là, soutenu que la loi « informatique et libertés » rendait une telle coordination plus difficile. Une telle affirmation est tout à fait inexacte.

Il doit être rappelé, à ce sujet, que les directions départementales d'action sanitaire et sociale sont chargées de tenir des fichiers informatiques pour assurer le suivi des personnes hospitalisées d'office en raison de troubles mentaux. Le préfet et les services placés sous son autorité chargés d'instruire les demandes de port d'armes sont bien sûr habilités à avoir accès, à cette occasion, aux informations détenues par les DDASS. Un décret du 7 mai 1995 prévoit d'ailleurs explicitement que les autorisations d'acquisition et de détention de port d'armes peuvent être retirées pour des raisons d'ordre public ou de sécurité des personnes, et fait obligation à chaque préfecture de mettre en œuvre un fichier des détenteurs d'armes, ces derniers devant informer le préfet du département de tout changement de domicile. La CNIL a autorisé la mise en oeuvre de tels fichiers tant par les DDASS pour les personnes hospitalisées d'office (délibération n° 94-024 du 29 mars 1994), que par les préfectures pour les détenteurs d'armes. Les uns et les autres sont bien évidemment accessibles au préfet et à ses services compétents. De surcroît, la Commission, saisie par le ministère de l'Emploi et de la Solidarité en décembre 1998 d'une demande de conseil sur l'accessibilité des fichiers des personnes internées d'office par les services de police dans le cadre de certaines procédures administratives, a clairement indiqué qu'aucune disposition de la loi du 6 janvier 1978, ni aucune de ses délibérations sur le sujet, ne s'opposait à ce que les fichiers des personnes hospitalisées d'office puissent être consultés par les services de police dans le cadre de la procédure d'autorisation d'un port d'arme, d'agrément des activités privées de surveillance, de gardiennage et de transports de fonds, ni dans le cadre de la délivrance du permis de conduire, un trouble mental ayant entraîné une hospitalisation d'office nécessitant d'ailleurs l'avis d'un psychiatre agréé, autre que celui qui a soigné le sujet, préalablement à la délivrance du permis de conduire. En revanche, le principe de finalité du fichier et celui de non-discrimination fondé sur l'état de santé des personnes a conduit la Commission à estimer que les procédures de regroupement familial et de naturalisation ne justifiaient pas, en l'état des textes en vigueur, la consultation du fichier des personnes hospitalisées d'office.

2 — LA POSSIBILITÉ DE CONSULTER, DANS LE CADRE DE CERTAINES ENQUÈTES ADMINISTRATIVES DE MORALITÉ, LES FICHIERS DE POLICE JUDICIAIRE OU DE GENDARMERIE

L'article 28 de la loi prévoit que les fichiers de police judiciaire, qu'ils soient mis en oeuvre par le ministère de l'Intérieur ou la Direction générale de la gendarmerie nationale, peuvent être consultés dans le cadre d'enquêtes administratives destinées à vérifier que le comportement des candidats n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées. Sont visées par ce texte les décisions administratives d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, lorsqu'elles concernent soit l'exercice de missions de sécurité ou de défense, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériel ou de produits dangereux. La loi précise en outre que ces consultations pourront porter sur des données relatives à des procédures judiciaires en cours.

Cette disposition législative met fin à un obstacle juridique que la CNIL ainsi que le Conseil d'État avaient relevé lors de l'examen du système de traitements des infractions constatées (STIC) mis en œuvre par le ministère de l'Intérieur. En effet, si la CNIL avait admis dans ses deux avis rendus sur le STIC *(cf.* 19e rapport d'activité pour 1998, p. 63 et 21e rapport d'activité pour 2000, p. *77)* que le fichier puisse être consulté par certains personnels de la police nationale, individuellement désignés et spécialement habilités par le directeur de la police national ou par le préfet, dans le cadre de missions de police administrative lorsque la nature de ces missions 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, elle s'était opposée à toute consultation d'un fichier de police judiciaire à l'occasion des enquêtes dites de moralité. La Commission avait en effet relevé que « la communication d'informations extraites de procès-verbaux de police judiciaire, dont le destinataire naturel est le procureur de la République, à des autorités administratives plusieurs années après l'établissement d'une procédure pénale, pourrait priver d'effet les dispositions [du code de procédure pénale régissant le casier judiciaire] qui énumèrent les condamnations dont la mention est exclue ou peut être effacée du bulletin n° 2, seul susceptible d'être exigé par les administrations publiques de l'Etat, notamment lors de certaines enquêtes administratives ». Elle avait en outre souligné « qu'en permettant à certaines autorités administratives d'avoir accès, par l'entremise du fichier, à des informations de police judiciaire, alors même que dans le cas où une condamnation serait finalement intervenue sur ces mêmes faits, la loi ou la juridiction saisie n'aurait pas permis qu'il en fût fait mention au bulletin n° 2, le dispositif proposé paraissait contraire à la volonté exprimée par le législateur ». Enfin, s'agissant des consultations opérées dans le cadre de certaines missions de police administrative, la Commission avait émis une réserve sur la possibilité de prendre ainsi connaissance d'informations relatives à des affaires en cours, ce qui lui paraissait contraire au secret de l'enquête et de l'instruction garanti par les dispositions de l'article 11 du code de procédure pénale.

C'est un nouvel équilibre entre les divers intérêts en cause que définit le dispositif arrêté par le législateur. La loi autorise ainsi désormais de telles consultations des fichiers de police judiciaire dans le cadre d'enquêtes administratives de moralité, mais elle en précise la portée.

En premier lieu, celles des enquêtes administratives pouvant donner lieu à la consultation des fichiers de police judiciaire sont, dans les limites déjà précisées par la loi (exercice de missions de sécurité ou de défense, accès à des zones protégées, utilisation de matériel ou produits dangereux) fixées par un décret en Conseil d'État (décret n° 2002-424 du 28 mars 2002, *JO* du 30 mars 2002, p. 5647).

En deuxième lieu, la loi prévoit que les consultations en cause devront être opérées « dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la nation ».

En troisième lieu et enfin, la loi du 15 novembre 2001 n'ayant pas entendu déroger aux dispositions générales de la loi du 6 janvier 1978, les modalités pratiques de telles consultations au bénéfice de nouveaux destinataires des informations

concernées devront être soumises à la Commission et les actes réglementaires relatifs aux fichiers en cause modifiés en conséquence.

3 — L'EXTENSION DU FICHIER NATIONAL AUTOMATISE DES EMPREINTES GÉNÉTIQUES

L'article 56 de la loi relative à la sécurité quotidienne a étendu le champ d'application du fichier national des empreintes génétiques à d'autres infractions que les seules infractions sexuelles initialement visées. Il concernera désormais également des crimes non sexuels : les crimes d'atteinte volontaire à la vie de la personne, de tortures et actes de barbarie et de violence volontaire sur mineurs ou personnes particulièrement vulnérables ayant entraîné une mutilation ou une infirmité permanente, les crimes de vols ayant entraîné une mutilation ou une infirmité permanente ou commis avec arme ou en bande organisée, les crimes d'extorsions avec violence et de destructions dangereuses pour les personnes ainsi que les crimes terroristes. Il est à relever qu'à ces divers titres, le fichier n'a pas été étendu aux simples délits.

Cependant, la loi sur la sécurité quotidienne a élargi la portée du fichier en matière d'infractions sexuelles dans le souci affiché de la protection des mineurs. Ainsi, elle prévoit désormais que seront également enregistrées dans le fichier national les empreintes génétiques des receleurs des infractions sexuelles visées par l'article 706-47 du code de procédure pénale. Sont principalement visées à ce titre les personnes se trouvant en possession d'images ou de vidéocassettes pédophiles.

Cette disposition résultant d'un amendement du gouvernement n'avait pas à recueillir l'avis de la CNIL qui a, en revanche, été saisie des modifications apportées au décret d'application du 18 mai 2000 qui avait mis en œuvre le fichier national. Les modifications apportées à ce décret étant de pure conséquence des dispositions législatives précédemment adoptées, la Commission a aussitôt donné un avis favorable.

Il convient de rappeler que les empreintes génétiques enregistrées dans le fichier ne concernent que des traces relevées sur les lieux du crime ou du délit et les empreintes génétiques des personnes définitivement condamnées pour l'une des infractions visées par la loi.

En outre, il sera relevé que la loi sur la sécurité quotidienne paraît mettre fin au principe de l'inviolabilité du corps humain auquel le code de procédure pénale n'apportait jusqu'à présent aucune dérogation dans la mesure où le refus par une personne définitivement condamnée de se soumettre à un prélèvement biologique destiné à l'inclure dans le fichier est désormais puni d'une peine de six mois d'emprisonnement et de 7 500 euros d'amende, et d'une peine aggravée lorsque l'infraction commise justifiant le prélèvement est un crime et non un délit.

4 — L'OBLIGATION FAITE AUX OPERATEURS DE TÉLÉCOMMUNICATIONS ET AUX INTERMÉDIAIRES TECHNIQUES DE L'INTERNET DE CONSERVER LES DONNÉES DE CONNEXION À DES FINS DE POLICE

Cette disposition, introduite par l'article 29 de la loi relative à la sécurité quotidienne dans le code des postes et télécommunications, a fait l'objet de très nombreux commentaires soulignant qu'elle serait directement liée aux événements du 11 septembre. Force est pourtant de constater que tel n'est pas le cas dans la mesure où, à la différence d'autres amendements finalement inclus dans le projet de loi sur la sécurité quotidienne, l'obligation faite aux intermédiaires techniques de communication de conserver les données de connexion à des fins de police figurait précédemment dans le projet de loi sur la société de l'information, préparé et rendu public bien antérieurement au 11 septembre. Ce projet de loi sur la société de l'information avait fait l'objet de nombreuses prises de position publiques et avait été soumis, pour avis, à la CNIL et au Conseil d'État. Sans doute, cependant, les événements du 11 septembre ont conduit le Gouvernement à accélérer le calendrier initialement prévu.

. La loi prévoit désormais que les données de connexion ne peuvent pas être conservées au-delà d'un an et renvoie à un décret en Conseil d'État pris après avis de la CNIL le détail de la durée de conservation selon les données en cause, connexion à Internet, données de localisation des téléphones portables, etc. La loi précise explicitement qu'en aucun cas les données conservées ne pourront permettre d'identifier la navigation d'un internaute mais il résulte du dispositif législatif que la police judiciaire pourra, en cas d'infraction et d'enquête, avoir accès aux données en cause.

Le 21e rapport d'activité pour 2000 avait très largement rappelé l'avis de la CNIL sur ce projet (p. 21, *sqq.).* Il peut ainsi être résumé.

La volatilité des informations numériques et la difficulté d'identifier les auteurs d'infraction qui peuvent agir dissimulés contraignent l'ensemble des États démocratiques à faire obligation aux fournisseurs d'accès à Internet de conserver pendant un temps déterminé les éléments permettant d'identifier les internautes en cause. Chacun paraît aujourd'hui s'accorder sur un tel objectif.

Toutefois, le caractère dérogatoire d'une telle mesure d'identification qui n'a été appliquée ni pour le minitel ni pour les autres moyens de télécommunication, impose de rechercher le juste équilibre puisqu'il s'agit de rien de moins que d'identifier tous les internautes se connectant à Internet pour poursuivre les agissements illégaux d'une infime partie d'entre eux.

La CNIL a observé que la majorité des pays européens qui ont imposé une telle obligation aux fournisseurs d'accès se sont arrêtés à des durées de conservation de l'ordre de trois mois (Allemagne, Pays-Bas, Finlande) à six mois (Suisse), certains imposant une durée plus courte (deux mois en République Tchèque), d'autres plus longues (au moins un an pour la Belgique).

Au fur et à mesure qu'une société s'informatise et que se généralise l'utilisation de moyens informatiques nomades (une carte bancaire, un téléphone mobile) ou

des architectures en réseau, les gisements de données ou les « traces informatiques » qui touchent nos activités se multiplient. Ces gisements de données constituent pour la police autant d'éléments de preuve aisément accessibles. Il s'agit d'en mettre de nouveaux à sa disposition. Un souci d'équilibre et de proportionnalité a convaincu la CNIL qu'une durée de conservation limitée à trois mois pour les données de connexion à Internet serait adaptée à l'ensemble des intérêts en cause. La Commission avait formé le vœu qu'une telle durée figurât dans la loi elle-même. Elle n'a pas convaincu le Gouvernement ni le Parlement, mais aura à examiner le projet de décret en Conseil d'État pris pour son application. À la date de rédaction du présent rapport, la CNIL n'a pas été saisie de ce projet de décret.

B. Droits des maladies : le renforcement de l'accès aux données

Réclamé depuis longtemps par les associations de malades, annoncé par le Premier ministre lors des États généraux de la santé en 1999, l'accès direct au dossier médical est désormais consacré par la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

Jusqu'à présent, quiconque voulait connaître le contenu de son dossier médical, qu'il soit ou non informatisé, devait passer par l'intermédiaire d'un médecin. L'article 40 de la loi du 6 janvier 1978, comme l'article 6 de la loi du 17 juillet 1978 ou encore l'article L. 1112-1 du code de la santé publique prévoyaient ainsi que le patient devait désigner un médecin de son choix pour obtenir communication de son dossier médical, à charge pour ce dernier d'apprécier, en conscience, celles des informations figurant dans le dossier médical qui pouvaient être portées à la connaissance du titulaire du droit d'accès.

La principale justification de cette intermédiation tenait au souci de protéger les malades contre toute réaction susceptible d'être provoquée par la révélation d'un pronostic grave ou fatal. S'y mêlait également le souci que la portée exacte des informations médicales soit bien comprise par le patient.

Cette approche est apparue, au fil du temps et des pratiques, révélatrice d'une conception de la médecine jugée un peu « paternaliste ».

Revendiquant désormais le droit d'être pleinement associés à la décision médicale, disposant aujourd'hui, grâce aux médias et aux sites Web, de multiples moyens de s'informer sur la pathologie dont ils souffrent, sur la technique chirurgicale utilisée pour leur opération, sur l'efficacité du traitement proposé, les malades attendent généralement de leurs médecins une information claire et complète sur leur état de santé et aspirent à une plus grande transparence de la part du corps médical.

Avec la nouvelle loi, quiconque souhaitera obtenir son dossier médical pourra soit, comme par le passé, désigner un médecin de son choix, soit en faire la demande directement auprès du médecin ou de l'établissement de santé qui détient le dossier.

La CNIL a bien entendu noté cette avancée pour les droits des malades.

Elle avait déjà, à plusieurs reprises, en particulier lors des différents avis rendus sur les expériences de cartes de santé et sur le volet médical de la future carte VITALE 2, mis l'accent sur la nécessaire évolution de notre droit en ce domaine. La CNIL avait ainsi estimé que la nécessité de recueillir l'accord des patients et de leur garantir la maîtrise des informations figurant sur la carte Vitale devait s'accompagner du droit d'en connaître le contenu, à charge pour le médecin par l'intermédiaire duquel la puce serait lue de donner toutes les explications nécessaires.

De même, dans son avis sur le projet de disposition législative instituant le volet de santé de la future carte VITALE 2[1] , la Commission avait estimé que l'usager devait se voir reconnaître le droit de consulter, sans restriction, l'intégralité du contenu de ce volet.

La Commission a, plus récemment, lors de l'examen de projets de dossiers de santé sur Internet, souligné le paradoxe, sinon la contradiction, qu'il y aurait à offrir à l'usager de santé les moyens de décider du support et des modalités de communication de son dossier de santé sans lui donner le droit d'avoir directement connaissance des informations y figurant.

Dès lors, la Commission ne pouvait qu'accueillir favorablement cette évolution du droit d'accès, tout en étant parfaitement consciente des risques que comporterait pour le patient la révélation sans aucune précaution d'information sur sa santé et des dérives qui pourraient résulter d'une trop grande transparence lorsque les informations en cause sont liées à un pronostic grave, aux caractéristiques génétiques, ou encore lors de la communication au profit de tiers de données médicales.

Aussi, la Commission a-t-elle approuvé la philosophie générale du texte qui lui a été soumis en juillet 2001 et en particulier les précautions prises pour aménager, dans certaines circonstances, la communication des données.

1 — LES « FILETS DE SÉCURITÉ » PRÉVUS

Il en est ainsi en particulier de la faculté laissée au médecin de recommander au patient, lors de la consultation de certaines informations, la présence d'une tierce personne, pour des motifs déontologiques tenant aux risques que leur connaissance sans accompagnement pourrait faire courir à la personne concernée.

Procède également de cette même prudence, la possibilité prévue par la loi, pour le médecin détenteur du dossier d'exiger la présence d'un médecin désigné par le demandeur lors de la consultation d'informations recueillies dans le cadre d'une hospitalisation psychiatrique d'office ou sur demande d'un tiers, et en cas de refus du demandeur, de saisir la commission départementale des hospitalisations psychiatriques dont l'avis prévaut alors.

Des précautions sont par ailleurs prises pour protéger les mineurs de certains comportements de leurs parents. Il est ainsi prévu qu'un médecin peut se dispenser du consentement des parents sur les décisions médicales à prendre lorsque le traitement

[1] Délibération du 18 février 1999.

ou l'intervention s'imposent pour sauvegarder la santé d'un mineur et que le mineur s'oppose expressément à ce que les titulaires de l'autorité parentale soient consultés. Cependant, la décision revient, en telle hypothèse, au professionnel de santé et non au mineur concerné.

Il est également prévu que lorsqu'une personne mineure, dont les liens de famille sont rompus, bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture maladie universelle, son seul consentement à l'intervention médicale suffise.

Dans son avis du 10 juillet 2001, la Commission avait suggéré qu'il soit prévu que, dans certaines hypothèses exceptionnelles, le mineur de plus de 16 ans puisse avoir accès à son dossier médical hors la présence de ses parents, mais en étant alors accompagné d'un médecin ou d'une personne majeure de son choix. La loi du 4 mars 2002 est demeurée silencieuse sur ce point. Toutefois, son décret d'application du 29 avril 2002 a tenu compte de la suggestion de la Commission. En effet, l'article 6 de ce décret prévoit que la personne mineure peut souhaiter garder le secret sur un traitement ou une intervention dont elle a fait l'objet, le médecin étant alors tenu de faire mention écrite de l'opposition du mineur à ce que ces informations soient communiquées aux titulaires de l'autorité parentale. Lorsque le médecin est saisi d'une demande de communication du dossier présentée par les parents, ce texte lui fait obligation de s'efforcer d'obtenir le consentement du mineur à la communication des informations en cause mais si, en dépit de ces efforts, le mineur maintient son opposition, la demande de la communication du dossier présenté par les titulaires de l'autorité parentale ne peut être satisfaite.

Enfin, s'agissant du droit d'accès des ayants droit au dossier médical d'une personne décédée, la loi prévoit désormais explicitement qu'ils pourront se voir délivrer, sur leur demande, des informations issues du dossier médical de la personne décédée lorsque ces informations sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. Sur ce point, la Commission se réjouit que les suggestions qu'elle avait faites dans son avis du 10 juillet aient conduit le Gouvernement à modifier son projet dans un sens moins restrictif à l'égard des ayants droit.

2 — LE DROIT À LA CONFIDENTIALITÉ RÉAFFIRMÉ

La loi réaffirme le droit pour toute personne au respect de sa vie privée et du secret des informations la concernant et oblige à cet effet les professionnels et établissements de santé à mettre en oeuvre des règles de confidentialité qui devront être définies par décret en Conseil d'État pris après avis public et motivé de la Commission nationale de l'informatique et des libertés.

La nécessité de prévoir des normes de sécurité obligatoires dans le domaine particulièrement sensible du traitement des données médicales répond au voeu de la CNIL. Qu'il s'agisse de la gestion des dossiers médicaux par le professionnel de santé ou de la transmission des données médicales par réseau aux caisses de Sécurité

sociale ou par l'intermédiaire d'organismes concentrateurs techniques ou encore dans le cadre de recherches ou de réseaux de santé, la CNIL a toujours souhaité que les mesures permettant de garantir la confidentialité des données médicales soient adaptées à l'évolution des normes techniques dans ce domaine.

Enfin, la Commission dans son avis rendu le 10 juillet 2001 a proposé que le projet de loi soit complété par une disposition interdisant toute exploitation commerciale des données de santé à caractère personnel, reprenant en cela sa recommandation du 8 mars 2001 sur les sites de santé dans laquelle elle avait émis le souhait que le principe de l'interdiction de toute commercialisation de données de santé directement ou indirectement nominatives soit posé dans la loi, à l'instar de ce qui est d'ores et déjà prévu par le code de la santé publique s'agissant des données relatives aux prescriptions des professionnels de santé lorsqu'elles revêtent un caractère directement ou indirectement nominatif.

Cette proposition n'a pas été retenue. En revanche, le Gouvernement a fait adopter, conformément au vœu exprimé par la CNIL, une disposition visant à encadrer l'activité des prestataires techniques appelés à héberger des données de santé, qu'il s'agisse de *données* collectées dans le *cadre de* sites Internet, de réseaux de soins ou encore de données rassemblées dans des dispositifs d'archivage des dossiers médicaux. Cette activité, encore balbutiante, et dont on ne sait d'ailleurs pas si elle trouvera son « marché », nécessite, en tout état de cause, compte tenu des risques potentiels de divulgation et d'exploitation commerciale des données inhérents à ce type de services, d'être étroitement encadrée. Un dispositif d'agrément est ainsi institué par la loi dont les modalités précises seront fixées par décret en Conseil d'Etat pris après avis de la CNIL.

Délibération n° 01-041 du 10 juillet 2001 portant avis sur le projet de loi de modernisation du système de santé

La Commission nationale de l'informatique et des libertés ; Saisie pour avis du projet de loi relatif à la modernisation du système de santé par le ministre délégué à la Santé ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de la santé publique ; Vu

le code de la Sécurité sociale ;

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

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu Monsieur Michel Gentot, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Le projet de loi soumis à l'examen de la Commission comporte trois titres consacrés respectivement à la démocratie sanitaire (titre I), à la qualité du système de santé (titre II) et aux dispositions relatives à l'outre-mer (titre III). La Commission a plus particulièrement examiné les dispositions relatives à l'interdiction de toute discrimination dans l'accès à la prévention ou aux soins (article L. 1112-2 nouveau du code de la santé publique), au droit d'accès aux données médicales (article L. 111 3-6 nouveau au code de la santé publique), aux mesures de confidentialité (article L. 1112-3 nouveau du code de la santé publique), au droit à l'information (article L. 1113-1 nouveau du code de la santé publique) ainsi que celles relatives à la création d'un office des professions paramédicales (article L. 4391-1 et suivants nouveaux du code de la santé publique).

Sur l'interdiction de toute discrimination dans l'accès à la prévention ou aux soins

L'article 2 du projet de loi (article L. 1112-2 nouveau du code de la santé publique) réaffirme le principe de l'interdiction de toute discrimination dans l'accès à la prévention ou aux soins en consacrant en particulier l'interdiction de toute discrimination en raison des caractéristiques génétiques de la personne ou en fonction de sa situation en matière de protection sociale. Les progrès de la génétique et du traitement de l'information peuvent en effet susciter de nouveaux risques d'exclusion professionnelle ou de stigmatisation sociale, telles que la révélation à des tiers des prédispositions génétiques à telle ou telle pathologie ou l'instauration de systèmes de protection sociale sélectifs.

Aussi, la Commission approuve-t-elle cette disposition qui est de nature à renforcer les droits fondamentaux des personnes et, en particulier, le droit à la santé tel qu'il est reconnu par le préambule de la Constitution de 1946.

Sur le droit d'accès direct aux données médicales

L'article 6 du projet de loi (article L. 1113-6 nouveau du code de la santé publique) dispose que toute personne peut accéder, directement ou par l'intermédiaire d'un praticien qu'elle désigne à cet effet, à l'ensemble des informations « formalisées » concernant sa santé détenues par des professionnels et établissements de santé ayant contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ayant fait l'objet d'échanges écrits entre professionnels.

L'article 7 du titre 1er du projet de loi prévoit en conséquence une modification de coordination de l'article 40 de la loi du 6 janvier 1978. Une volonté accrue de transparence des patients à l'égard de leurs données de santé, l'émergence de nombreuses sources d'informations médicales, et tout particulièrement de sites de santé destinés au grand public sur Internet, et les récentes dispositions légales relatives au volet médical de la carte de santé qui subordonnent tout enregistrement de données de santé au consentement exprès des personnes concernées justifient la reconnaissance d'un droit d'accès direct par l'usager à ses informations de santé.

La Commission estime toutefois que les risques que pourrait comporter la révélation sans aucune précaution d'informations liées à un pronostic grave ou

aux caractéristiques génétiques de la personne, ou ceux qui pourrait résulter d'un détournement du droit d'accès direct afin d'exiger de l'intéressé, dans des circonstances étrangères à la relation de soins, la production d'un « certificat de bonne santé » doivent être pesés et pris en compte.

Aussi la Commission approuve-t-elle les mesures prévues par le projet de loi et en particulier la faculté laissée au médecin de recommander, lors de la consultation de certaines informations, la présence d'une tierce personne pour des motifs déontologiques tenant aux risques que leur connaissance sans accompagnement pourrait faire courir à la personne concernée (3e alinéa de l'article L. 1113-6 nouveau du code de la santé publique).

De même, elle prend acte du délai prévu pour assurer la communication des informations, qui ne pourrait intervenir qu'au plus tard dans les huit jours à compter de la demande, et au plus tôt après qu'un délai de réflexion de quarante-huit heures aura été observé.

Enfin, elle prend acte que le projet de loi renvoie à un décret en Conseil d'Etat le soin de déterminer les mesures d'application de cet article.

Sur le cas particulier des mineurs

L'article 6 du projet de loi (alinéa 6 de l'article L. 1113-6 nouveau du code de la santé publique) prévoit que le droit d'accès des mineurs sera *exercé* par le ou les représentants de l'autorité parentale, le mineur pouvant cependant demander que l'accès puisse avoir lieu par l'intermédiaire d'un médecin désigné par le ou les titulaires de l'autorité parentale.

La Commission estime qu'un dispositif devrait être mis en place permettant à un mineur désirant garder le secret sur son état de santé d'exercer lui même son droit d'accès, au moins pour les mineurs âgés de plus de 16 ans. Dans une telle hypothèse, le projet de loi pourrait prévoir que le mineur devrait se faire accompagner par un médecin ou une personne majeure de son choix.

Un tel dispositif serait seul de nature à éviter qu'un mineur, redoutant d'éventuelles réactions des responsables de l'autorité parentale liées à la révélation de son état de santé, renonce à exercer le droit d'accès direct qui est désormais reconnu à tous les patients.

Une disposition de cette nature s'inscrirait dans la droite ligne des dispositions récemment adoptées par le Parlement relatives à l'interruption volontaire de grossesse et à la contraception.

Sur le cas particulier des ayants droit d'une personne décédée

L'article 6 (alinéa 7 de l'article L. 1113-6 nouveau du code de la santé publique) prévoit qu' « en cas de décès du malade, ses ayants droit peuvent accéder, sur leur demande, aux seuls éléments du dossier nécessaires pour leur permettre de défendre la mémoire du défunt ou de faire valoir leurs droits. Cet accès ne peut avoir lieu si le défunt a exprimé une volonté contraire. » Si la consécration par le projet de loi d'un droit de communication au bénéfice des ayants droit d'une personne décédée recueille l'assentiment de la Commission, la rédaction proposée, en ce qu'elle limite les éléments du dossier communicable « aux seuls éléments... nécessaires pour leur permettre de défendre la mémoire du défunt ou de faire valoir leurs droits », paraît tout à la fois restrictive et de nature à engendrer des interprétations délicates. Aussi, la Commission est-elle d'avis que cette restriction soit levée.

Sur la confidentialité des données médicales et les mesures de sécurité

L'article 2 du projet de loi (article L. 1112-3 nouveau du code de la santé publique) rappelle le principe de la confidentialité des données médicales (toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant), tout en consacrant la pratique du « secret médical partagé » au bénéfice du patient (lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe). La Commission accueille favorablement ces dispositions dans la mesure où elles permettent, dans l'intérêt de l'usager, une meilleure coordination des soins entre les membres de l'équipe soignante.

La Commission prend également acte que des dispositions autorisent certaines catégories de professionnels de santé, dans le cadre de leurs missions, à accéder aux informations couvertes par le secret médical : médecins conseils du contrôle médical des organismes d'assurance maladie et personnes placées sous leur autorité, praticiens experts de l'Agence nationale d'accréditation des établissements de soins, membres des commissions de conciliation instituées dans les établissements de santé, membres de l'inspection générale des affaires sociales.

Par ailleurs, le projet de loi renvoie à un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés le soin de déterminer les règles de conservation sur support informatique et de transmission par la voie électronique des données médicales ainsi que la détermination des cas dans lesquels l'utilisation de la carte électronique individuelle mentionnée à l'article L. 161-33 du code de la sécurité sociale serait rendue obligatoire.

Compte tenu du caractère technique et rapidement évolutif des mesures de sécurité en matière de traitement de l'information à caractère personnel, le renvoi de la définition de règles générales de sécurité à un décret en Conseil d'État ne paraît pas adapté, l'application des règles issues de la loi du 6 janvier 1978 ou de celles qui résulteront de la transposition de la directive européenne du 24 octobre 1995 paraissant davantage de nature à prendre en compte la diversité et la spécificité des traitements d'informations en cause.

Sur la reconnaissance d'un droit général à l'information

L'article 6 du projet de loi (alinéa 1er de l'article L. 1113-1 nouveau du code de la santé publique) dispose que « toute personne doit, sauf en cas d'urgence ou d'impossibilité, être informée sur son état de santé, sur les différentes investigations, traitements ou actions de prévention qui lui sont proposés, leur utilité, leur urgence éventuelle, leurs conséquences, les risques fréquents ou graves normalement prévisibles qu'ils comportent, ainsi que sur les solutions alternatives et sur les conséquences prévisibles en cas de refus ». L'alinéa 2 de cet article précise que « cette information, due par tout professionnel de santé dans le cadre de ses compétences, est délivrée au cours d'un entretien individuel » et qu'« elle doit être intelligible, loyale et adaptée à son destinataire. Elle doit être délivrée préalablement à l'expression du consentement aux soins et doit être renouvelée aussi souvent que nécessaire. Elle ne peut être refusée au motif du secret médical ».

En outre, la nécessité de procéder à cette information est complétée par l'article 6 du projet de loi (article L. 1113-3 nouveau du code de la santé publique) qui dispose que « toute personne prend, compte tenu des informations et préconisations des professionnels de santé, les décisions concernant sa santé. Aucun acte, aucun traitement ne peut être décidé et pratiqué sans son consentement libre et éclairé ».

La Commission, soucieuse qu'une information claire et précise soit donnée aux usagers du système de santé, ne peut qu'accueillir favorablement le renforcement des obligations des professionnels de santé en ce domaine.

Sur la création d'un office des professions d'infirmier, masseur-kinésithérapeute, orthophoniste, orthoptiste et pédicure-podologue

L'article 50 du projet de loi (article L. 4391-1 nouveau du code de la santé publique) prévoit une nouvelle organisation de certaines professions paramédicales par la création d'un office spécifique à ces professions exercées en France à titre libéral ; cette disposition instaure en particulier une procédure d'inscription à un fichier professionnel dont les conditions d'application seront fixées par décret en Conseil d'État.

Il devrait être prévu que ce décret sera pris après avis de la Commission nationale de l'informatique et des libertés.

Pour une interdiction de toute exploitation commerciale des données personnelles de santé.

Le développement d'offres de services à caractère commercial en matière de traitement de l'information de santé, l'apparition d'organismes intermédiaires chargés d'assurer la transmission par la voie électronique de données de santé et la création de nombreux sites Web spécialisés dans l'information médicale et collectant des données personnelles, doivent conduire à une grande vigilance à l'égard des exploitations possibles d'informations à caractère personnel révélant l'état de santé.

Compte tenu de la nature particulière des données de santé qui relèvent de l'intimité de la vie privée, et des risques d'exclusion que la connaissance de telles données est susceptible de présenter pour les personnes concernées, le projet de loi devrait être complété par une disposition interdisant toute commercialisation des données de santé directement ou indirectement nominatives, ainsi que le code de la santé publique l'a déjà prévu s'agissant des données relatives aux prescriptions des professionnels de santé lorsqu'elles revêtent à leur égard un caractère directement ou indirectement nominatif (article L. 4113-7 du code de la santé publique).

La Commission, qui a déjà exprimé ce voeu dans sa délibération n° 01-011 du 8 mars 2001, estime que la philosophie générale du texte qui lui est présenté devrait conduire à y inclure une disposition de cette nature.

En conséquence :

Approuve la proposition de modification de l'article 40 de la loi du 6 janvier 1978 tendant à reconnaître un droit d'accès direct des personnes aux informations médicales.

Demande :

— qu'un dispositif soit prévu, permettant aux mineurs âgés de plus de 16 ans désirant garder le secret sur leur état de santé d'exercer directement leur

droit d'accès, accompagnés par un médecin ou une personne majeure de leur choix ;

— que, s'agissant du droit de communication aux ayants droit du dossier d'une personne décédée, la limitation de ce droit aux seuls éléments du dos sier nécessaires pour leur permettre de défendre la mémoire du défunt ou de faire valoir leurs droits soit supprimée ;

— que la référence à un décret en Conseil d'État pris après avis de la Com mission nationale de l'informatique et des libertés s'agissant des règles tech niques de sécurité relatives à la conservation sur support électronique des informations médicales comme de leur transmission par voie électronique soit supprimée ;

— qu'il soit prévu que le décret en Conseil d'État fixant les conditions de tenue du fichier des professions paramédicales soit pris après avis de la Commission nationale de l'informatique et des libertés ;

— que le projet de loi soit complété par une disposition interdisant toute commercialisation des données de santé à caractère personnel, comme est déjà interdite par le code de la santé publique l'utilisation à des fins de pros pection commerciale des données relatives aux prescriptions des médecins lorsqu'elles revêtent à leur égard un caractère directement ou indirectement nominatif.

C. Prospection directe : les ordonnances des 25 juillet et 23 août 2001

Deux ordonnances des *15* juillet et 23 août 2001 ont transposé en droit français les dispositions de deux directives européennes[1] relatives aux secteurs des télécommunications et de la vente à distance.

Ces ordonnances interdisent l'envoi de télécopies ou l'utilisation d'automates d'appels à des fins de prospection à l'égard des personnes qui n'y auraient pas préalablement consenti.

Depuis de nombreuses années, la CNIL porte sur le secteur du marketing direct une attention vigilante. Qu'il soit prospecté par un automate programmé pour l'appeler sur son téléphone ou sur son télécopieur, l'usager considère, à juste titre, que ces modes d'intervention sont particulièrement intrusifs.

Les premières réclamations dont la Commission a été saisie se rapportaient à la prospection par automates d'appels téléphoniques. De nombreux consommateurs exaspérés refusaient d'être sans cesse dérangés par des appels répétés, le plus souvent en début de soirée, de voix robotisées leur vantant les mérites des produits les plus divers. La CNIL a réagi dès 1985 en adoptant une recommandation préconisant que la diffusion de messages téléphoniques par automates d'appels soit subordonnée à l'accord préalable et exprès des personnes appelées. Très rapidement, la plupart des professionnels ont renoncé, en France, à ce mode de prospection : aujourd'hui, la Commission n'est plus saisie de réclamations en cette matière.

[1] Directive 97/66 du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécoms et directive 97/7 du 20 mai 1997 concernant la protection des consommateurs en matière de contrat à distance.

La prospection par télécopie a cependant pris la relève.

Ce mode de prospection s'adresse principalement aux usagers, personnes physique ou morale, abonnés au service de télécopie pour des besoins professionnels : il s'agit, dans le langage du marketing, de « *business to business* » ou « *B to B* ».

Désormais, ce sont des médecins, des architectes, des artisans, des agriculteurs, des prêtres, des gérants d'entreprises, des trésoriers d'associations, des proviseurs de lycée qui recevant quotidiennement des dizaines de télécopies publicitaires[1] saisissent la CNIL. La plupart manifestent leur exaspération de ne plus pouvoir utiliser leur télécopieur très souvent bloqué par la réception de ces messages. Plusieurs centaines de réclamations parviennent chaque année à la CNIL à ce sujet.

Le législateur est intervenu une première fois en 1989. La loi a alors donné la possibilité aux abonnés à la télécopie de s'inscrire sur une liste, dénommée « liste safran », afin de s'opposer à recevoir des télécopies à caractère publicitaires. Ces dispositions étaient assorties de sanctions pénales, tout démarchage publicitaire effectué par télécopie à l'égard d'une personne inscrite en « liste safran » depuis plus de deux mois étant punie de l'amende prévue pour les contraventions de troisième classe, pour chaque message expédié, soit 450 euros.

Cependant, plus de 10 ans après sa création, force est de constater que la liste d'opposition n'a pas fonctionné. De nombreux opérateurs de marketing ne l'ont pas respecté et ont continué à prospecter par télécopie des abonnés qui avaient pourtant pris le soin de s'inscrire sur la « liste safran ». Le nombre de plaintes reçues par la Commission dans ce secteur, sans cesse en augmentation, en témoigne nettement.

Les ordonnances des *25* juillet et 23 août 2001 sont venues sanctionner cette situation. Désormais, le principe est simple : l'envoi par télécopie ou par automate d'appels de messages publicitaires est interdit en France (comme dans l'ensemble des États membres de l'Union européenne) sauf à l'égard des personnes qui auraient spécialement exprimé leur consentement à être ainsi démarchées. Un registre est prévu, dans lequel ces dernières peuvent s'inscrire si elles souhaitent être prospectées par ce biais. Il n'est pas besoin de préciser qu'à ce jour, ce registre n'a guère rencontré de succès !

Un nouvel article (L. 33-4-1) inséré dans le code des postes et télécommunications interdit « la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels ».

Le code de la consommation interdit parallèlement « la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels » (nouvel article L 121-20-5).

[1] Article R. 10-2 du code des postes et télécommunications.

Il doit être souligné que ces textes visent « la prospection directe » et non le seul démarchage commercial. La prospection à des fins politique, associative, religieuse ou caritative est dès lors concernée par ces nouvelles dispositions, comme la Commission l'avait souhaité.

S'agissant des sanctions pénales, un projet de décret, qui a été soumis pour avis à la Commission, prévoit que tout message de prospection adressé en infraction à ces dispositions sera puni d'une amende de 1 500 euros.

Sans attendre la publication de ce décret, la CNIL intervient systématiquement auprès des sociétés qui adressent des télécopies publicitaires lorsque la prospection a été envoyée, par ce moyen, à une personne physique. La Commission ne dispose en effet d'aucune compétence pour agir lorsqu'elle est saisie par une personne morale.

Le domaine de la prospection par télécopie ou par automates d'appels est donc désormais réservé aux relations entre un professionnel et son client ou son correspondant qui, à l'occasion de la conclusion d'un contrat par exemple, aura donné son accord pour recevoir des télécopies publicitaires. En outre, dans des circonstances particulières qui ne relèvent pas de la « prospection », l'usage des automates d'appels n'est pas interdit. Tel peut être le cas d'opérateurs d'urbanisme ou de collectivités locales qui souhaitent informer, par ce biais, les citoyens de travaux imminents, de changements de trajets de bus, de coupures d'eau ou d'électricité, etc.

L'exigence du consentement préalable dans le domaine de la prospection par télécopie ou par automates d'appels constitue un véritable changement, en France, pour les professionnels du marketing direct qui devraient tirer les enseignements des choix législatifs successifs intervenus dans ce secteur.

Dès aujourd'hui, d'autres modes de prospection font l'objet d'une attention particulière de la part de la CNIL : il s'agit de la prospection par mél ou par *Short Message Service (SMS)*.

L'ordonnance du 23 août 2001 évoque ces autres « techniques de communication à distance » (la prospection par voie postale, par téléphone, par mél et par SMS), l'article L. 121-20-5 du code de la consommation disposant que « lorsqu'elles permettent une communication individuelle, les communications à distance [autres que les automates d'appel et les télécopieurs] ne peuvent être utilisées que si le consommateur n'a pas manifesté son opposition ».

Il demeure que la prospection par mél est encore en débat en France, en Europe et aux USA. Pour ce qui la concerne, la CNIL en reste aux conclusions qu'elle a adoptées et rendues publiques dans son rapport intitulé te *publipostage électronique et la protection des données personnelles.*

La Commission a souhaité que les conditions dans lesquelles peut s'effectuer un publipostage électronique soient appréciées au regard des moyens utilisés par le site pour collecter l'adresse électronique de l'internaute.

Ainsi, un site peut régulièrement adresser un courrier électronique à un internaute qui lui aura volontairement fourni son adresse mél, qu'il soit client, prospect ou

visiteur. Le site doit cependant informer les personnes concernées de leur droit de s'opposer à de tels envois et indiquer très clairement le moyen d'exprimer cette opposition qui doit pouvoir intervenir à tout moment.

Le publipostage électronique est également régulier, au regard de la loi du 6 janvier 1978, s'il est effectué à partir à partir d'une liste de méls fournie par un tiers, mais à la condition que l'internaute ait été préalablement informé de la mise à disposition de son adresse électronique à des tiers (partenaires commerciaux, autres filiales d'un même groupe, etc.) et mis en mesure de s'y opposer par un moyen simple et gratuit, tel qu'une case à cocher prévue à cet effet sur le formulaire initial de collecte.

Le véritable problème posé par le publipostage électronique est en effet celui de la capture sauvage d'adresses dans les espaces publics d'Internet, « chats », forums, annuaires, listes de diffusion, à partir desquels les méls peuvent être techniquement collectés sans que les personnes concernées en aient connaissance. De telles pratiques sont irrégulières.

Dans un communiqué de presse diffusé en ligne le 4 décembre 2001, la CNIL a rappelé que le publipostage électronique effectué à partir d'adresses capturées sur Internet à l'insu des personnes concernées lui paraissait impropre à assurer la protection des données personnelles, le respect de la vie privée et la tranquillité des internautes.

III. LA TRANSPOSITION DE LA DIRECTIVE DU 24 OCTOBRE 1995

La transposition de la directive du 24 octobre 1995 a enfin connu une première étape législative importante : le projet de loi, adopté en Conseil des ministres après consultation de la CNIL et avis du Conseil d'État, a fait l'objet d'un premier vote à l'Assemblée nationale le 30 janvier 2002 et a été adopté sans modifications substantielles par rapport aux grandes orientations gouvernementales qui avaient été exposées dans le précédent rapport d'activité (21^{e} rapport d'activité pour 2000, p. 17).

Toutefois, certaines dispositions nouvelles qui ont été introduites au cours de ces premiers débats parlementaires, méritent d'être présentées.

Les « cookies »

Le projet comporte désormais des dispositions spécifiques sur Internet, et tout particulièrement sur les « cookies », introduites à l'article 5 (article 32 nouveau — I bis de la loi du 6 janvier 1978). Ces dispositions ont fait l'objet de nombreux commentaires et, semble-t-il, d'importantes discussions avec les professionnels concernés. Elles précisent que l'utilisation des réseaux en vue de stocker des informations dans le terminal d'un internaute (le disque dur), ou d'accéder à des informations

ainsi préalablement stockées dans le terminal (la lecture d'un « cookie » précédemment stocké), n'est autorisée que si l'internaute a été préalablement informé de manière « claire et complète » des finalités du « cookie » et des moyens de s'y opposer. Elles interdisent par ailleurs de subordonner l'accès à un service Web à l'acceptation des « cookies », et ménagent des dérogations lorsque le « cookie » a pour seule finalité d'assurer la sécurité d'une connexion, ainsi par exemple, l'accès à une messagerie distante.

Ces dispositions consacrent la doctrine développée par la CNIL qui n'avait pas estimé utile de suggérer qu'elles soient consacrées au niveau législatif. L'amendement initialement présenté s'inspirait de très près d'un amendement que le Parlement européen avait adopté à l'occasion de la révision de la directive relative à la protection des données personnelles en matière de télécommunications. L'amendement discuté devant le Parlement européen avait pour objet d'interdire que des informations puissent être stockées dans l'équipement terminal, d'un abonné, ainsi que tout accès à des informations stockées dans ce terminal sans le consentement préalable de la personne concernée. Cette disposition visait à interdire les logiciels espions et ne pouvait, à ce titre, qu'être approuvée. Cependant elle conduisait également à soumettre au consentement préalable de l'internaute l'usage des « cookies ». Dans sa généralité, une telle disposition ne paraissait pas adaptée, ce qui a conduit la CNIL à diffuser un communiqué de presse le 7 décembre 2001 sur cette question.

S'il est vrai, en effet, que certains usages de cette technologie, notamment aux Etats-Unis, ont pu susciter de légitimes inquiétudes il y a quelques années, la réaction des internautes et des autorités de protection des données ont largement permis de les apaiser. Ainsi, les navigateurs les plus répandus permettent, grâce à un paramétrage très simple à mettre en œuvre, d'être systématiquement informé de l'envoi d'un « cookie » et de s'y opposer. Ils permettent également de refuser systématiquement tout « cookie ». Enfin, à la différence des données personnelles enregistrées sur le serveur d'un tiers, les « cookies » qui ne peuvent être lus que par son émetteur peuvent être effacés par l'internaute de son disque dur. La rubrique « Vos traces sur Internet » sur www.cnil.fr donne les précisions utiles à cet égard.

La CNIL a rappelé que la plupart des « cookies » jouent le rôle de simples « témoins de connexion » destinés à faciliter la navigation sur un site Web ou à sécuriser l'accès (à sa messagerie électronique par exemple) sans avoir à ressaisir des informations identifiantes, et qu'elle recommandait depuis juillet 1998 que le site émetteur informe les internautes de la finalité des « cookies », de leur durée de validité s'ils ne sont pas effacés par l'internaute à l'issue de la session, et des conséquences de la désactivation de ces procédés. Elle indiquait qu'une information claire et complète sur ces points était seule de nature à apaiser les inquiétudes trop souvent encore entretenues par un regrettable défaut de transparence.

En définitive, la Commission considère comme satisfaisante la rédaction d'équilibre finalement retenue, à ce stade de la procédure parlementaire, par l'Assemblée nationale.

LE DROIT DES HERITIERS SUR LES DONNEES A CARACTERE PERSONNEL DE LEURS PARENTS DECEDES

Une disposition spécifique a été introduite dans l'article 40 nouveau relative au droit d'accès et de rectification des héritiers d'une personne décédée. Cette disposition prévoit que les héritiers peuvent exiger du responsable du traitement qu'il « prenne en considération le décès » et procède aux « mises à jour qui doivent en être la conséquence ». Il est par ailleurs précisé que les héritiers qui « ont exercé la faculté prévue à l'alinéa précédent » sont en droit d'interroger le responsable du traitement afin « d'obtenir la confirmation que les données à caractère personnel concernant le défunt font, ou non, encore l'objet d'un traitement ».

Les débats parlementaires ne permettent pas en l'état de parfaitement mesurer la portée de cette disposition qui peut être interprétée de deux manières très différentes, sinon divergentes. À préciser ainsi certains droits particuliers des héritiers, le projet tel qu'il a été adopté entend-t-il cantonner le droit des héritiers aux seuls droits d'accès et de mise à jour, en les excluant du droit à l'information préalable, du droit d'opposition pour raison légitime et du droit de radiation ? Dans une telle hypothèse, cette disposition aurait un avantage : lever un délicat problème d'interprétation sur le point de savoir si les données à caractère personnel relatives à une personne décédée sont ou non incluses dans le champ d'application de la loi, c'est-à-dire bénéficient ou non d'une protection ; elle aurait un inconvénient : priver toute personne vivante de la protection des données personnelles relatives à un proche décédé (père, mère, conjoint, descendant, etc.), alors qu'il pourrait être soutenu que l'ayant droit est particulièrement concerné, fût-ce indirectement par le sort, l'usage, la divulgation de telles données. Il convient de relever que la directive européenne du 24 octobre 1995 est silencieuse sur ce point, et il reste à espérer que la poursuite des débats parlementaires pourra lever toute ambiguïté sur la portée de la disposition en cause.

LE DISPOSITIF PARTICULIER REGISSANT LES TRAITEMENTS DE DONNÉES AUX FINS DE JOURNALISME

L'article 67 nouveau de la loi (article 11 du projet adopté par l'Assemblée nationale) n'a pas été modifié au cours des débats parlementaires mais a fait l'objet, une fois son adoption en première lecture acquise, de commentaires souvent très vifs.

L'objectif poursuivi par ce texte vise à concilier les principes fondamentaux de protection des données personnelles et la liberté d'expression. Déjà, la loi du 6 janvier 1978 avait ménagé, dans son article 33, certaines dérogations au bénéfice des organismes de presse écrite et audiovisuelle. Ainsi, la presse est libre de transmettre toutes données nominatives à l'étranger, même si l'organisme destinataire des données n'assure pas un niveau de protection équivalent ou adéquat, libre de collecter et traiter les informations relatives aux infractions, condamnations et mesures de sûreté (normalement réservées aux seuls organismes en charge d'un service public de justice ou de police), libre de collecter et traiter des données sensibles

(normalement soumises à un régime de garantie renforcée). Il en allait de la liberté de la presse et de la libre communication des idées.

La CNIL a très clairement manifesté, et de longue date, le vœu que ces dérogations soient étendues et a mené, dès 1995, une large concertation avec de nombreux organismes de la presse nationale et régionale, à l'issue de laquelle elle a rendu une recommandation spécifique à ce domaine d'activité (16e rapport d'activité pour 1995, p. 27). En effet, à appliquer strictement et sans mesure les règles et principes de la loi du 6 janvier 1978 aux activités de presse, le souci de l'équilibre manifesté par la loi du 29 juillet 1881 sur la liberté de la presse serait entamé. En tout état de cause, il convenait de prévenir tout détournement des textes qui aurait par exemple, à l'heure de la numérisation des activités concernées, permis à un particulier de tenter de s'opposer à la parution d'un article le concernant au motif qu'il aurait été préparé ou stocké sur un support informatique ou, de manière plus générale, de jouer de la loi « informatique et libertés » contre la loi sur la presse.

Aussi, la CNIL s'est-elle efforcée, dans sa recommandation de 1*995,* de définir un équilibre entre les grands principes généraux de la loi « informatique et libertés » et les spécificités, constitutionnellement protégées, de la liberté d'expression et de la communication.

La directive du 24 octobre 1995 n'a pas fait autre chose en prévoyant, dans son article 9, que les États-membres devaient prévoir, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exceptions et dérogations « dans la mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ».

La transposition de la directive a conduit le Gouvernement à élargir le nombre et la portée des dérogations au bénéfice, notamment, des organismes de presse. Outre celles déjà prévues par la loi du 6 janvier 1978, ces organismes seraient purement et simplement dispensés de l'obligation d'information préalable, de l'obligation de répondre à d'éventuelles demandes de droit d'accès ou de rectification (irrecevables à leur égard) et de l'obligation de déclarer leurs traitements de données à caractère personnel mis en œuvre au titre de l'activité journalistique, la seule contrepartie à cette dernière dispense consistant à désigner un « responsable à la protection des données » chargé de tenir un registre des traitements mis en oeuvre. Cette dernière disposition relative à la désignation par l'organisme de presse lui-même d'un « correspondant à la protection des données » est apparue, à tort ou à raison, porteuse de risque pour la liberté de la presse.

La suite de l'examen du projet de loi pourrait permettre de lever toute ambiguïté ou quiproquo sur le sens de cette disposition. Il n'est pas douteux qu'en cette matière le seul contrôle de l'activité de presse doit être un contrôle *a posteriori,* comme le prévoient les dispositions de la loi de juillet 1881, et ne doit nullement s'apparenter à une quelconque forme de censure préalable.

À cet égard, le dernier alinéa du texte voté précise que sont applicables les dispositions du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal « qui prévoient les conditions d'exercice du droit de réponse et

préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée ou à la réputation des personnes ». Une interprétation a *contrario* signifie, certes implicitement mais nécessairement, qu'aucun des droits reconnus par la loi « informatique et libertés » aux personnes concernées par un traitement de données personnelles ne pouvait trouver à s'appliquer à l'égard d'un document numérique tant que ce dernier n'a pas fait l'objet d'une publication ou d'une diffusion.

Il convient enfin de relever que la désignation par les organismes de presse d'un « délégué à la protection des données personnelles » devant principalement tenir registre des traitements mis en œuvre à des fins de journalisme — ces traitements n'ayant plus alors à être notifiés à la Commission — avait été recommandée par la CNIL en 1995, et avait paru recueillir l'assentiment des organismes de presse consultés sur ce point.

Il est vraisemblable que la suite de la procédure parlementaire permettra de revenir sur l'ensemble de ces points délicats.

LE RENFORCEMENT DES PENALITES REPRIMANT LES INFRACTIONS À LA LOI « INFORMATIQUE ET LIBERTÉS »

La CNIL avait regretté que le projet de loi de modification de la loi du 6 janvier 1978 abaisse les pénalités réprimant les infractions à la protection des données personnelles. Elle ne peut que se réjouir que le débat à l'Assemblée nationale ait permis, à ce stade de la procédure parlementaire, de les rétablir et de les mettre en cohérence, les valeurs à protéger n'étant pas de moindre importance aujourd'hui qu'il y a vingt ans.

UN RENFORCEMENT DU CONTROLE DES ENREGISTREMENTS VISUELS DE VIDÉOSURVEILLANCE MIS EN ŒUVRE DANS LES LIEUX PUBLICS ET OUVERTS AU PUBLIC

La loi du 21 janvier 1995 ayant mis en oeuvre un dispositif particulier régissant la vidéosurveillance des lieux publics et ouverts au public a été complétée pour prévoir que le Gouvernement transmettrait chaque année à la CNIL un rapport faisant état de l'activité des commissions départementales, présidées par un magistrat de l'ordre judiciaire, et chargées d'émettre un avis destiné au préfet du département, auquel revient le soin d'autoriser ou non les dispositifs concernés. Cette disposition est de nature à assurer une meilleure information du public sur l'évolution du recours à de tels dispositifs.

Le débat parlementaire n'est pas achevé. La première lecture du texte a cependant paru manifester un assez large consensus sur le dispositif tel qu'il a été arrêté par le Gouvernement après une très longue phase de consultation et de réflexion. Il reste à souhaiter que la France puisse disposer, maintenant sans tarder, d'une loi actualisée et modernisée.

Chapitre 2

LES INTERVENTIONS DE LA CNIL

Le présent chapitre évoque quelques grands domaines d'intervention de la CNIL en 2001. Délibérations portant avis sur des projets de traitements publics, suites à donner à des missions de contrôles sur place, recommandations dans certains secteurs particuliers d'activité ou rapports d'ensemble sur telle question d'intérêt général, ce chapitre illustre la variété des modes d'intervention de la CNIL et dégage des éléments de doctrine dont la connaissance paraît plus particulièrement utile à une bonne application de la loi du 6 janvier 1978[1].

I. LE SORT DES FICHIERS DE CLIENTELE LORS DES FUSIONS D'ENTREPRISES

Les données personnelles ont acquis une valeur marchande et constituent une richesse de l'entreprise. Comment protéger les données à caractère personnel lors des fusions ou des acquisitions d'entreprises ? C'est une question qui se pose de manière concrète dans tous les pays du monde et à peu près dans les mêmes termes.

Aux États-Unis, une décision judiciaire relative au sort du fichier de clientèle de la filiale en faillite d'un groupe a eu un fort retentissement. Cette affaire est connue sous le nom de « Toysmart », filiale du groupe Walt Disney qui vendait en ligne sur Internet des jouets pour les enfants. Lors de la faillite de cette filiale, le problème s'est

[1] D'autres délibérations importantes ont davantage trouvé leur place dans le chapitre 3 du présent rapport consacré aux « débats en cours ». C'est notamment le cas des avis rendus par la CNIL en matière d'administration électronique, et tout particulièrement de la mise en place par les administrations financières des premières phases opérationnelles du système Copernic.

posé de savoir si le fichier de clientèle pouvait ou non être considéré comme un actif cessible de l'entreprise. Saisie par plusieurs associations de consommateurs, la Cour des faillites de Boston a relevé, d'une part, que les clients de « Toysmart » n'avaient pas été informés lors de leurs achats que leurs coordonnées étaient susceptibles d'être utilisées par d'autres sociétés, d'autre part, que les données à caractère personnel en cause concernaient des mineurs, spécialement protégés par la loi dite « COPPA » *(cf.* VI. L'Internet et les mineurs). Aussi, la juridiction a-t-elle confirmé l'accord finalement passé entre la filiale et la maison mère stipulant que le fichier en cause, loin de pouvoir être utilisé par d'autres que « Toysmart », devait être purement et simplement détruit, le groupe Walt Disney devant régler le coût des opérations de destruction.

Les législations européennes de protection des données à caractère personnel s'inspirent d'une philosophie semblable même si, en pratique, leur application permet d'éviter des solutions aussi radicales que la destruction d'un fichier.

La saisine de la Commission par un parlementaire relative au sort du fichier de clientèle de Canal+ lors de la fusion des sociétés Vivendi, Seagram et Canal+ a conduit la Commission à préciser certains éléments de doctrine et à inciter Canal+ à renforcer les mesures d'information des personnes sur leurs droits.

A. La saisine de la Commission et la mission de vérification sur place

Un parlementaire abonné à Canal+ a saisi la CNIL au mois de décembre 2000 en faisant valoir qu'il n'avait accepté de figurer dans le fichier des abonnés que dans le seul but de recevoir des programmes télévisés et qu'il n'entendait pas que ses coordonnées soient livrées à des tiers pour un usage différent.

La Commission a décidé, lors de sa séance plénière du 16 janvier 2001, de procéder à une mission de vérification sur place auprès de Canal+ afin de s'assurer de l'effectivité des engagements souscrits par cette société à l'occasion des formalités déclaratives de son fichier des abonnés accomplies en 1993 et 1998.

La mission de vérification qui s'est déroulée le 6 février 2001 a permis de s'assurer des conditions de fonctionnement du fichier des abonnés de Canal+, de la pertinence des informations qui y étaient enregistrées, ainsi que des éventuelles conditions d'utilisation de ces données par d'autres filiales du groupe à des fins de prospection.

Les investigations de la Commission n'ont pas établi qu'il ait été fait par Canal+ ou d'autres sociétés du groupe un usage des informations nominatives contraire aux dispositions de la loi. La délégation de la Commission s'est par ailleurs assurée qu'un mécanisme d'identification était mis en place par Canal+ pour garantir le droit de tout abonné de s'opposer à la cession de ses coordonnées à des tiers. Un indicateur, géré par le service informatique, est en effet affecté aux personnes ayant manifesté leur droit d'opposition.

Mais les vérifications menées ont eu essentiellement pour effet de s'assurer de la complète information des personnes concernées sur leurs droits.

B. Les liens capitalistiques entre entités juridiques distinctes sont sans incidence sur le droit des personnes concernées

Contrairement à une idée commune, la loi « informatique et libertés », pas davantage que la directive européenne, n'interdit la cession ou la mise à disposition de fichiers privés à des fins commerciales au profit d'entreprises tierces. La vente, la location, la mise à disposition de fichiers de données personnelles n'est nullement interdite et correspond à un secteur d'activité toujours croissant. Internet a illustré ce phénomène, et chacun a pu constater que certains sites Web à vocation commerciale étaient mis en place, moins dans le souci de vendre un produit ou un service que dans celui de constituer un fichier de visiteurs ou d'acheteurs qui pourra ensuite être vendu à un tiers, à un coût d'autant plus élevé, que le « profil » commercial des visiteurs ou acheteurs sera précis.

En revanche, toute personne a le droit de s'opposer à la cession de ses données à des tiers à des fins d'exploitation commerciale et aucune disposition de la loi du 6 janvier 1978 ou de la directive européenne du 24 octobre 1995 ne limite ce droit : les personnes doivent être préalablement explicitement informées de l'éventualité d'une telle cession et mises en mesure de s'y opposer.

À cet égard, les liens de capital qui peuvent exister entre l'entreprise qui cède son fichier et l'entreprise cessionnaire sont sans incidence sur le droit pour les personnes concernées de s'opposer à une telle cession. La CNIL l'affirme avec clarté dans sa délibération « la circonstance que ces tiers [les entreprises cessionnaires] soient devenus des entités juridiques distinctes au sein d'un même groupe est, à cet égard, indifférent et ne saurait priver les personnes des droits qu'elles tiennent de la loi de protection des données personnelles, au motif de l'évolution de liens capitalistiques caractérisant le co-contractant ».

En vertu du principe de finalité des fichiers, un groupe capitalistique réunissant des entités juridiquement distinctes dont certaines peuvent exercer des activités tout à fait différentes ne saurait, au seul motif des liens du capital, mêler dans un même ensemble des bases de données constituées pour des fins différentes, sans souci du droit que les personnes tiennent des législations de protection des données personnelles de s'y opposer. Les fusions entre entreprises ne peuvent pas conduire à une interconnexion généralisée de leurs fichiers.

C. Le droit de s'opposer à la cession de ses données à des fins de prospection doit être effectif ; la condition de cette effectivité est une parfaite information des personnes concernées

Tel est le deuxième intérêt de la délibération relative à la mission de vérification sur place effectuée auprès de canal+.

En effet, si les cessions de données personnelles ne sont pas interdites, que les données soient cédées à une autre filiale d'un même groupe ou à une entreprise

tout à fait étrangère au capital du responsable du fichier en cause, c'est à la condition que les personnes concernées aient été préalablement informées d'une telle éventualité et mises en mesure de s'y opposer, simplement et gratuitement.

Encore convient-il que cette information soit faite clairement et n'apparaisse pas comme une clause de style. À cet égard, la CNIL a demandé à Canal+ de prendre diverses mesures afin de mieux informer les personnes de leurs droits et de faciliter, le cas échéant, l'exercice du droit d'opposition. Il doit être relevé que la Commission a tout spécialement demandé à Canal+ de veiller à ce que la police de caractère utilisée pour les mentions d'informations spécifiques « informatique et libertés » soit d'une taille raisonnable, élément qui confirme la vigilance de la Commission sur le caractère effectif de l'information du consommateur, telle qu'elle avait été précédemment exprimée, notamment dans sa délibération n° 97-012 du 18 février 1997 portant recommandation relative aux bases de données comportementales sur les habitudes de consommation des ménages constituées à des fins de marketing direct (18e rapport d'activité, p. 53).

Le même souci d'effectivité des mesures prises ou à prendre a conduit la Commission à fixer une clause de rendez-vous avec Canal+, six mois plus tard.

Il a été vérifié à cette date que les engagements pris par Canal+ avaient été tenus. Ainsi, Canal+ a publié dans les numéros de juillet/août 2001 et septembre 2001 de son magazine mensuel des programmes, distribué à tous les abonnés par la voie postale, une rubrique d'information rappelant les droits d'accès, de rectification et d'opposition à la communication d'informations à d'autres sociétés. Une rubrique spécifique permettant que le droit d'opposition puisse s'exercer directement en ligne, depuis le service minitel ou le site Web de Canal+ a été créée et les nouveaux contrats d'abonnement à Canal+ comportent les mentions CNIL modifiées avec ajout d'une case à cocher pour que les abonnés futurs puissent manifester directement leur opposition à cession, qu'il s'agisse des contrats réseau, par correspondance ou câble opérateur. Enfin, Canal+ a indiqué qu'aucune utilisation du fichier de ses abonnés au bénéfice d'autres filiales du groupe n'avait été effectuée en 2001.

Délibération n° 01-040 du 28 juin 2001 relative à la mission de vérification sur place effectuée auprès de Canal+

La Commission nationale de l'informatique et des libertés ;

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 directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21 ;

Vu le décret n° 78-774 du 17 juillet 1978, pris pour l'application de la loi susvisée ;

Vu le règlement intérieur de la Commission et notamment ses articles *55* et *56* ;

Vu la convention du 8 décembre 2000 entre Canal+ SA et Canal+ Distribution ;

Vu la déclaration par Canal+ du traitement de gestion de la clientèle n° 358437 ;

Vu la plainte n° 00017325 en date du 19 décembre 2000 et les correspondances afférentes ;

Vu la délibération n° 01-001 du 16 janvier 2001 décidant une mission de vérification sur place auprès de Canal+ ;

Vu le rapport relatif à la mission de contrôle adressé par lettre du 1er juin 2001 et les observations en réponse de Canal+ reçues par lettre du 21 juin 2001 ;

Après avoir entendu Madame Cécile Alvergnat et Monsieur Didier Gasse, commissaires, en leur rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Commission a été saisie le 19 décembre 2000 d'une réclamation relative à l'utilisation qui pourrait être faite du fichier des abonnés de la société Canal+, dans le cadre de l'opération Vivendi Universal, nouveau groupe né de la fusion des sociétés Vivendi, Seagram et Canal+, effective depuis le 8 décembre 2000.

Le plaignant précisait qu'il n'avait accepté de figurer dans le fichier d'abonnés que dans le seul but de recevoir des programmes télévisés et qu'il n'entendait pas que ses coordonnées soient mises à la disposition de tiers pour un usage différent.

La Commission a décidé, lors de sa séance plénière du 16 janvier 2001, de procéder à une mission de vérification sur place auprès de Canal+ afin de s'assurer de l'effectivité des engagements souscrits par cette société à l'occasion des déclarations déposées à la CNIL en 1984, 1993 et 1998 et de vérifier les conditions d'utilisation à des fins commerciales pour le compte de tiers, des données relatives *aux* abonnés. Cette mission s'est déroulée à partir du 6 février 2001.

La nature et l'organisation de la base des abonnés à Canal+

Le fichier des abonnés à Canal+ se présente sous la forme classique d'un fichier de clientèle. Il comporte les informations relatives au contrat d'abonnement (coordonnées de l'abonné et éventuellement du tiers offrant l'abonnement, options choisies, mode de règlement, références bancaires pour les prélèvements automatiques ainsi que toutes les données relatives à la gestion de l'abonnement) mais aussi les informations collectées auprès des abonnés à l'occasion des enquêtes de satisfaction auxquelles procède régulièrement l'opérateur, ainsi que des informations relatives aux services associés, offerts par Canal+, tels que le « forum boutique » qui permet de passer des commandes de téléachat ou le « service Kiosque » qui permet de sélectionner un bouquet de programmes (football, saison de formule 1, OMTV, playboy TV) ou encore les services dits « à la demande » *(pay per view).*

Il doit être relevé que, s'agissant du téléachat, aucune donnée relative aux commandes passées par les clients ne figure dans la base de données dite « des abonnés ». S'agissant de l'utilisation des services à la demande, la conservation sous la seule forme d'un numéro associé au programme acheté a pour finalité exclusive le règlement des contestations possibles, étant observé qu'un système de jetons prépayés permet, pour certaines catégories de films, de regarder un programme sans que ce dernier puisse être identifié. Il a été indiqué qu'aucune exploitation commerciale de ces informations n'est effectuée et que de manière générale, aucune information sur les programmes regardés n'est disponible par retour d'informations à partir des décodeurs.

En revanche, la délégation de la Commission a noté que le système de gestion de la clientèle regroupait au sein d'une même base de données tous les abonnés et anciens abonnés, qu'il s'agisse des abonnés à Canal+ quel que soit le vecteur de réception de la chaîne (voie hertzienne, câble, ou satellite) ou des abonnés à CanalSatellite dont 80 % sont communs à Canal+.

L'utilisation du fichier des abonnés de Canal+ à des fins de prospection commerciale pour le compte de tiers

Le principe

Les cessions ou mises à disposition de fichiers privés à des fins commerciales au profit d'entreprises tierces ne sont pas interdites par la loi du 6 janvier 1978 ou par la directive européenne du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données, sous réserve de l'application de législations spéciales pouvant offrir des garanties supplémentaires. Cependant, et conformément aux articles 25, 26 et 27 de la loi, de telles cessions ou mises à disposition seraient irrégulières en l'absence d'information préalable des personnes concernées, qui doivent également être mises en mesure de s'y opposer gratuitement et sur simple demande de leur part.

Les situations successives de Canal+ en la matière

La société Canal+ a procédé en 1984 à la déclaration de son traitement de gestion des abonnés, sous la forme d'une déclaration simplifiée en référence à la norme 25 (gestion des fichiers de destinataires d'une publication périodique de presse). Le contrat passé entre les abonnés et Canal+ indiquait à l'époque que l'abonnement restait strictement confidentiel entre l'abonné et Canal+ d'où il résultait qu'en aucun cas les données relatives aux abonnés ne pouvaient être mises à la disposition de tiers.

En 1993, Canal+ a procédé à une nouvelle déclaration auprès de la CNIL indiquant que son fichier d'abonnés pourrait être mis à disposition de toutes autres sociétés du groupe pour l'envoi de documents de prospection. La Commission avait alors attiré l'attention de Canal+ sur la nécessité que les abonnés soient, conformément à la loi, informés de l'éventualité de telles cessions commerciales au bénéfice de tiers et mis en mesure de s'y opposer. Canal+ avait alors complété ses contrats d'abonnement par une mention spécifique pour satisfaire à cette exigence.

Cette déclaration a été modifiée par Canal+ en 1998 afin d'intégrer de nouvelles utilisations en matière de prospection commerciale, et tout particulièrement une utilisation du fichier des abonnés à des fins de prospection commerciale pour le compte de sociétés n'appartenant pas au groupe. Le contrat d'abonnement a été modifié en conséquence pour permettre aux nouveaux abonnés d'être informés d'une telle éventualité et de leur droit de s'y opposer.

Enfin, à la fin de l'année 2000 et dans le cadre du rapprochement entre Canal+ SA et les sociétés Vivendi SA et The Seagram Company Ltd, Canal+ SA s'est engagé à apporter la quasi totalité de ses actifs et passifs à une nouvelle entité dénommée « groupe Canal+ », détenue à 100 % par le nouvel ensemble Vivendi Universal, à l'exclusion notamment de la propriété de la base d'abonnés à la chaîne. Aux termes de la convention signée entre Canal+ SA et Canal+ Distribution le 8 décembre 2000, si Canal+ SA demeure propriétaire de la base d'abonnés, Canal+ Distribution, filiale à 100 % du groupe Canal+, a la jouissance exclusive de la base d'abonnés pour tous usages commerciaux autres que la distribution et la commercialisation de la chaîne, ce qui signifie tout particulièrement que les usages du fichier des abonnés à Canal+ à des fins de prospection commerciale au bénéfice des autres entités du groupe ou de tiers au groupe relèveront de la responsabilité de Canal+ Distribution et non pas de Canal+ SA. La convention passée entre les deux entités stipule cependant que Canal+ SA sera préalablement informée de tout projet d'utilisation de la base d'abonnés à de telles fins et disposera, dans certaines conditions, d'un droit d'opposition à *ces* projets.

Les constatations de la Commission

Les investigations menées par la Commission n'établissent pas que le fichier des abonnés de Canal+ ait été utilisé de façon non conforme à la loi du 6 janvier 1978 s'agissant des mises à disposition au bénéfice de tiers depuis janvier 1998, date avant laquelle tout délit serait prescrit.

S'agissant de la plainte reçue par la CNIL le 19 décembre 2000, il n'est ni soutenu ni établi que les données concernant le plaignant telles qu'elles figurent dans le fichier des abonnés de Canal+ aient été utilisées pour le compte de tiers. La délégation de la Commission a pu constater que cet abonné a été identifié dans le fichier, depuis la réception de sa plainte, comme s'opposant à toute cession d'informations le concernant à des tiers. Un indicateur, géré par le système informatique, est affecté aux personnes qui ont manifesté ce souhait et deux codes sont utilisés à cette fin, l'un pour les abonnés de Canal+, l'autre pour les abonnés de CanalSatellite.

S'agissant de la situation nouvelle créée par le rapprochement décidé entre Canal+ SA et le groupe Vivendi Universal, qui s'est traduit par une convention conclue le 8 décembre 2000, les représentants de Canal-t- ont indiqué que le fichier des abonnés n'a pas, depuis cette date, fait l'objet d'une utilisation au bénéfice d'une autre entité juridique du groupe Vivendi Universal, ni au bénéfice d'un tiers. Aucun élément matériel n'a été réuni par la Commission permettant de contester ces affirmations, la décision de la Commission de procéder à une mission de vérification sur place étant, par ailleurs, intervenue le 16 janvier 2001, soit cinq semaines seulement après la signature de la convention.

Les mesures à prendre pour assurer la protection des données personnelles des abonnés de Canal+

La convention conclue entre Canal+ SA et Canal+ Distribution précise dans son article 4-3 que les parties agiront dans le strict respect des dispositions de la loi du 6 janvier 1978. Le respect de la loi « informatique et libertés » implique cependant la mise en oeuvre de mesures concrètes à défaut desquelles le dispositif d'ensemble tel qu'il a été arrêté ne permettrait pas une utilisation régulière du fichier des abonnés de Canal+ pour le compte de tiers.

En effet, les personnes qui se sont abonnées à Canal+ jusqu'à 1993 n'ayant pas été informées de l'éventualité que les informations les concernant seraient un jour susceptibles d'être utilisées par d'autres entités juridiques que Canal+ ni, a fortiori, mises en mesure de s'y opposer, les données les concernant ne sauraient, en l'état, être utilisées à des fins de prospection commerciale pour le compte de tiers. La circonstance que ces tiers soient devenus des entités juridiques distinctes au sein d'un même groupe est, à cet égard, indifférente et ne saurait priver les personnes des droits qu'elles tiennent de la loi de protection des données personnelles, au motif de l'évolution de liens capitalistiques caractérisant le co-contractant.

S'agissant des abonnés de 1994 à mai 1998 qui ont, eux, été informés par contrat de l'éventualité d'une cession de leurs données à des fins de prospection commerciale au sein du groupe Canal+ et mis en mesure de s'y opposer, les changements intervenus depuis lors ne permettent pas de considérer que ceux d'entre eux qui n'auraient pas, à l'époque, manifesté d'opposition à la cession à d'autres sociétés du groupe Canal+ feraient aujourd'hui le même choix alors que les données les concernant pourraient désormais être utilisées à des fins de prospection par des entités juridiques nouvelles poursuivant une activité sociale sans lien direct avec la diffusion de programmes audiovisuels. En outre, ces abonnés n'ont pas été informés d'éventuelles cessions à des sociétés extérieures au groupe.

S'agissant des personnes abonnées postérieurement à juin 1998, l'information sur d'éventuelles cessions à des tiers et leur droit de s'y opposer a été formellement faite, notamment sur les contrats. Toutefois, la police de caractère utilisée dans certains contrats ne permet pas raisonnablement de considérer que cette information a été effective à l'égard de l'ensemble des personnes concernées.

Aussi, Canal+, à l'issue des investigations menées par la Commission, a-t-il inséré dans son magazine mensuel des programmes qui est distribué individuellement par la voie postale (n° 6 de juillet-août 2001) une rubrique d'information rappelant l'existence du droit d'accès, de rectification et d'opposition à la communication d'informations à d'autres sociétés. Cette rubrique précise les modalités pratiques d'exercice de ces droits en renvoyant notamment aux services « Canal+ service consommateurs », à « l'espace clients » accessible par minitel ou par Internet. Il est en outre précisé que les frais d'envoi seront remboursés sur demande aux personnes ayant exercé ces droits.

Canal+ s'engage à renouveler cette opération d'information dans l'édition suivante du magazine.

En outre, Canal+ s'est engagé à faire figurer, sur le kiosque minitel et sur son site Internet, au côté de la mention d'information relative au droit d'opposition à cession, une case à cocher destinée à faciliter l'exercice de ce droit, conformément aux préconisations habituelles de la Commission en la matière.

Enfin, les différents modèles de contrat d'abonnement seront modifiés afin, d'une part, de recourir à une police de caractère qui soit de nature à tenir les personnes concernées pour raisonnablement informées de leurs droits et, d'autre part, d'y faire figurer une case à cocher permettant à toutes les personnes qui le souhaiteront de s'opposer dès la conclusion du contrat à la cession de leurs données à des tiers (que ces tiers soient ou non liés par les liens du capital au groupe Vivendi Universal). La refonte du contrat d'abonnement devrait intervenir avant le 1er septembre 2001.

L'ensemble de ces mesures nouvelles est de nature à permettre de considérer que tous les abonnés de Canal+ seront raisonnablement informés d'une éventuelle utilisation des données les concernant par d'autres entités du groupe ou par des tiers ainsi que de leur droit de s'y opposer. Il convient toutefois, ainsi que Canal+ s'y est engagé, que toute utilisation du fichier des abonnés à Canal+ à des fins de prospection commerciale pour le compte de tiers autres que Canal+ SA soit différée jusqu'au 1er octobre 2001 de sorte que les personnes concernées aient pu effectivement prendre connaissance de la nouvelle situation et de leurs droits et aient pu les exercer.

Enfin, ces mesures d'informations ne pouvant pas toucher les personnes qui ne sont plus à ce jour abonnées à Canal+ mais dont les coordonnées peuvent être régulièrement conservées dans le fichier, en aucun cas les informations les concernant ne pourront être cédées à quelque tiers que ce soit. Enfin la Commission prend acte que la seule finalité des cessions envisagées sous les garanties et aux conditions ci-dessus rappelées est la prospection commerciale, à l'exclusion de toute mise à disposition de données relatives aux abonnés pour une autre finalité, au bénéfice d'une société extérieure, qu'elle soit liée ou non par des liens de capital.

La durée de conservation des informations

La Commission a constaté que des informations relatives à des personnes qui n'étaient plus abonnées depuis plus de 10 ans ont été conservées dans la base de données. Il n'est cependant pas établi que ces informations aient fait l'objet d'une quelconque utilisation. Canal+ a pris l'engagement de procéder à l'effacement de toutes les informations concernant ces abonnés avant la fin 2001.

S'agissant en outre des services à la demande *(pay per view),* la Commission prend note que la seule information figurant dans la base des abonnés est le numéro de programme à l'exclusion de toute indication sur le titre de ce programme et qu'il existe au surplus un système de jetons prépayés pour certaines catégories de films. Elle prend note que Canal+ ni aucun tiers ne fait de ces données ou des informations relatives aux services de kiosque une exploitation à des fins de ciblage ou d'établissement de profils de consommation. Compte tenu toutefois du caractère particulier de ces données qui relèvent du secret des programmes prévu par la loi du 30 septembre 1986 relative à la liberté de communication, il y a lieu de rappeler que ces données ne peuvent être conservées que pendant la durée de contestation de la facturation.

Émet les conclusions suivantes :

Sur l'utilisation, par des sociétés tierces et à des fins de prospection commerciale, des informations sur les abonnés de Canal+

La Commission rappelle que de telles utilisations ne sont pas interdites par la loi du 6 janvier 1978 dès lors que les personnes concernées ont été informées de l'éventualité de la cession de ces données à d'autres sociétés et mises en mesure de manière effective de s'y opposer sur simple demande et gratuitement.

La Commission prend acte des engagements pris par Canal+, à l'issue de la mission de vérification sur place, à savoir :

— la publication dans le magazine mensuel des programmes qui est distribué à tous les abonnés par la voie postale d'une rubrique d'information rappelant les droits d'accès, de rectification et d'opposition à la communication d'informations à d'autres sociétés, dans les numéros de juillet/août 2001 et septembre 2001 ;

— la création d'une rubrique spécifique permettant que le droit d'opposition puisse s'exercer en ligne, depuis le service minitel ou le site Web ;

— pour les abonnés futurs, l'insertion dans les contrats d'une nouvelle mention d'information offrant aux abonnés la faculté d'exercer leur droit d'opposition directement au moyen d'une case à cocher ;

— l'utilisation d'une taille raisonnable de police des caractères utilisée pour les mentions d'information quel que soit le support de collecte utilisé, en particulier pour les contrats « Canal+ analogique ».

Ces engagements satisfont aux prescriptions de la loi, sous réserve qu'aucune exploitation de la base des abonnés à Canal+ ne soit effectuée, en dehors de son utilisation pour les besoins propres de la chaîne, jusqu'au 1er octobre 2001, afin de laisser aux abonnés le temps de réagir et de manifester, le cas échéant, leur opposition à la cession et que les informations relatives aux personnes désabonnées ne soient pas utilisées pour le compte de sociétés tierces.

Sur le secret des programmes choisis par les abonnés

Les dispositions de l'article 3 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication n'autorisant la levée de ce secret que si le consentement des personnes est recueilli, la Commission prend acte de ce que Canal+ déclare ne procéder à aucune analyse de ces consommations et *a fortiori* ne les cède à quiconque et demande que la durée de conservation des informations relatives au paiement à la séance et aux services kiosque soit limitée à la durée de contestation de la facturation.

Sur la durée de conservation des informations

Les informations relatives aux personnes qui ne sont plus abonnées depuis plus de dix ans devront être radiées de la base des abonnés d'ici la fin de l'année 2001.

La Commission fixe à Canal+ et à Canal+ Distribution **une clause de rendez-vous** au mois de décembre 2001 pour s'assurer de l'effecfivité de la mise en œuvre des mesures prises par Canal+ Distribution et Canal+ SA en application de la présente délibération.

II. DONNEES PERSONNELLES DES LOCATAIRES DE LOGEMENTS SOCIAUX

À la suite de diverses plaintes dont elle avait été saisie, la Commission a souhaité entreprendre une étude d'ensemble sur les informations collectées par les organismes de logements sociaux auprès des candidats à un logement. La demande de renseignements portant sur leur « origine » a tout particulièrement alarmé les personnes concernées et certaines associations de défense des Droits de L'Homme, notamment SOS Racisme.

La CNIL a rendu compte dans son 21e rapport d'activité pour 2000 des premiers enseignements tirés des missions de contrôle sur place auprès de trois organismes de logement social. Elle a décidé, en 2001, de prolonger ses contrôles par des missions de vérification auprès de onze bailleurs sociaux.

A. Les missions de vérification sur place

Le choix des organismes contrôlés a été guidé par le souci de l'équilibre et de la diversité. Ainsi, ont été retenus des organismes différents dans leur forme juridique (société anonyme d'HLM, office public d'habitations à loyer modéré, office public d'aménagement et de construction, logement foyer, société d'économie mixte, collecteur du 1 % patronal), situés à Paris, Lyon, Marseille, Nîmes, Bordeaux et dans le département de la Seine-Saint-Denis.

À la suite de ces missions, un certain nombre d'enseignements communs ont pu être relevés.

L'objectif de la mixité sociale n'est pas, à l'heure actuelle, atteint en France en matière de logements sociaux. Les interlocuteurs de la Commission soulignent que les conditions économiques et sociales de certains quartiers à fort taux de population immigrée aboutissent en définitive à renforcer une certaine forme de « ghettoisation », les habitants antérieurs les désertant peu à peu, et le personnel de gardiennage s'y faisant plus rare.

Les commissions d'attribution des logements sociaux sont généralement appelées à avaliser les propositions faites par le bailleur à l'issue d'une procédure qui privilégie le contact direct avec les candidats présentés: Alors que des critères généraux de priorité en faveur des personnes mal logées ou défavorisées sont fixés au plan départemental, il apparaît que l'appréciation du gardien de la résidence,

l'avis du « commercial » à la recherche des candidats, l'existence d'un précédent locataire dans les relations du candidat constituent des éléments bien plus décisifs que les informations administratives collectées et traitées par ordinateur.

La nationalité des candidats locataires est systématiquement recueillie en tant qu'élément d'état civil, les bailleurs précisant que cette information peut avoir des incidences sur la nature du titre de séjour à produire, élément indispensable pour les candidats de nationalité étrangère. Cependant, il est généralement souligné que la nationalité en tant que telle est moins importante au regard de l'objectif de mixité sociale que d'autres éléments tels que la date d'arrivée en France des candidats locataires étrangers, laquelle peut s'avérer utile pour déterminer les efforts d'accompagnement ou apprécier la capacité d'intégration des personnes concernées.

Enfin, les missions de vérification ont permis de constater l'usage fréquent dans les systèmes d'informations mis en place dans le cadre de l'attribution de logement de zones blocs notes, aussi appelées « commentaires » ou de « texte libre » qui permettent aux responsables de la gestion locative d'annoter ou d'enregistrer des appréciations sur le candidat locataire ou sur le locataire en place. La collecte libre des informations ainsi enregistrées présente le risque que certaines expressions retenues soient inadaptées, voire excessives, et en cela non conformes aux dispositions de la loi « informatique et libertés ».

B. Les enseignements de ces missions

Aucune infraction aux dispositions de la loi du 6 janvier 1978 n'a été relevée au cours de ces missions de vérification sur place. De manière plus générale, il peut être affirmé que les systèmes d'information mis en place par les organismes sociaux et la collecte de la nationalité des demandeurs paraissent, à l'issue de ces missions, étrangers à d'éventuelles discriminations en matière d'attribution de logements sociaux.

Toutefois, certaines pratiques sont de nature à susciter l'inquiétude des demandeurs de logement en alimentant des suspicions de discrimination à leur égard. Tel est particulièrement le cas des interrogations répétées ou trop fréquentes sur la nationalité des locataires. Ainsi, les enquêtes triennales d'occupation et les enquêtes de supplément de loyer solidarité ne doivent pas, au regard des textes législatifs et réglementaires qui les régissent, conduire à collecter des informations sur la nationalité des locataires ou des occupants des logements.

De même, toute interrogation sur « les origines » des candidats aux logements est dépourvue de pertinence et susceptible d'entamer le pacte républicain en distinguant entre Français ou en donnant l'impression qu'il serait procédé à une telle distinction.

Enfin, certaines dérives précédemment constatées (cf. 21^{e} rapport d'activité pour 2000, p. 48 et suivantes) ont conduit la Commission à préciser que le lieu de naissance, élément d'état civil au même titre que la date de naissance, ne pouvait justifier aucune sélection, ni enregistrement dans une rubrique autre que celle consacrée aux éléments de l'état civil.

Un souci de clarté a conduit la Commission à rappeler l'ensemble de ces recommandations dans une délibération unique sur le sujet.

Délibération n° 01-061 du 20 décembre 2001 portant recommandation relative aux fichiers de gestion du patrimoine immobilier à caractère social

La Commission nationale de l'informatique et des libertés ; Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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 de données à caractère personnel ;

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

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu la délibération n° 97-005 du 21 janvier 1997, modifiée par la délibération n° 01-062 du 20 décembre 2001, concernant les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social ;

Après avoir entendu Monsieur Guy Rosier, Commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, Commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Par délibération du 26 mai 1981, la Commission a souhaité faciliter les formalités déclaratives des organismes de gestion du patrimoine immobilier à caractère social en adoptant une norme simplifiée de déclaration applicable aux traitements de gestion de ces organismes.

Par délibération du 16 octobre 1984, la Commission a autorisé que soit collectée, dans le cadre de cette procédure simplifiée de déclaration, l'information relative à la nationalité des personnes concernées afin de mettre en œuvre les mécanismes de subventions destinés alors à inciter à la construction de logements réservés aux personnes immigrées et à permettre aux organismes concernés de veiller à ce que l'attribution des logements sociaux puisse assurer une « mixité sociale », reflet de la conception républicaine de la vie sociale.

Par délibération du 21 janvier 1997, la Commission, saisie par les organismes concernés, a admis que l'information relative à la nationalité des intéressés puisse être communiquée, dans le cadre de cette procédure simplifiée de déclaration, aux instances participant à l'attribution des logements sociaux. Saisie de plaintes pouvant laisser supposer que la collecte d'une telle information était susceptible de susciter certains préjugés défavorables, sinon des discriminations, la Commission a procédé à plusieurs vérifications sur place auprès d'organismes de gestion du patrimoine immobilier à caractère social répartis sur tout le territoire, en application de l'article 21 de la loi du 6 janvier 1978.

Aucun élément de fait n'atteste, en l'état, que les fichiers manuels ou informatisés mis en oeuvre dans le cadre du logement social et dont le fonctionnement a été vérifié par la Commission, soient susceptibles de générer ou de faciliter des discriminations.

Les enseignements de ces missions paraissent toutefois devoir conduire à rappeler certaines recommandations destinées aux responsables des traitements d'informations nominatives concernés.

1) Aucune information faisant apparaître directement ou indirectement les origines raciales, au sens de l'article 31 de la loi du 6 janvier 1978, des per sonnes concernées, ne saurait être collectée auprès des demandeurs de lo gement. Par ailleurs, aucune information relative aux « origines » du demandeur ou au pays de naissance de ses parents n'est pertinente au re gard de la finalité de tels traitements.

2) L'information relative à la nationalité des demandeurs de logement est un élément d'état civil, qui peut être régulièrement collecté et enregistré dans un traitement automatisé de gestion locative sociale et porté à la connaissance des instances participant à la procédure d'attribution.

3) Le lieu de naissance est, au même titre que la date de naissance, un élé ment d'état civil. La finalité des traitements de gestion des demandes de lo gements sociaux ne saurait justifier qu'un tri puisse être opéré sur le critère du lieu de naissance des intéressés, ni que l'information relative au lieu de naissance soit enregistrée de manière spécifique, c'est-à-dire ailleurs que dans les champs d'informations consacrés aux éléments d'état civil.

4) La date d'arrivée en France ne constitue pas, aux termes de la loi du 29 juillet 1998 relative à la lutte contre les exclusions et des plans départe mentaux d'action sociale, un critère devant être pris en compte pour appré cier l'ordre de priorité de l'examen de la demande. Si cette information est susceptible de déterminer des mesures particulières d'accompagnement so cial au bénéfice des personnes concernées, sa collecte systématique ne de vrait pas aboutir à ce que les étrangers séjournant depuis peu de temps sur le territoire français soient systématiquement tenus pour non prioritaires par chacun des organismes auxquels ils s'adressent. En tout état de cause, la norme simplifiée n° 20 ne prévoit pas la collecte de l'information relative à la date d'arrivée en France dans le cadre de cette procédure simplifiée de déclaration.

5) Une fois le locataire dans les lieux, il apparaît sans utilité au regard de la finalité des traitements de gestion mis en oeuvre de procéder à des interroga tions fréquentes sur la nationalité des intéressés. En tout état de cause, Tes textes législatifs et réglementaires régissant les enquêtes d'occupation des logements sociaux et les enquêtes de supplément de loyer solidarité ne men tionnent pas la nationalité parmi les informations pouvant être collectées. Aussi, la collecte de cette information, à l'occasion de ces enquêtes, auprès du titulaire du bail ou des personnes vivant dans les lieux, doit-elle être consi dérée comme excessive et dépourvue de pertinence au regard de la loi du 6 janvier 1978.

6) Toute information enregistrée dans les zones en texte libre, dites « blocs-notes », des traitements automatisés de gestion du patrimoine doi vent être pertinentes, adéquates et non excessives au regard de la finalité du traitement. Ces informations qui doivent être objectives et ne résulter d'au cun jugement de valeur porté sur les intéressés doivent leur être communi-

quées, au même titre que toute information les concernant, à l'occasion de l'exercice de leur droit d'accès.

7) Les candidats à la location d'un logement social et les locataires doivent être informés, de manière claire et intelligible, du caractère obligatoire ou facultatif des réponses, des conséquences à leur égard d'un défaut de réponse, des destinataires des informations, et du lieu où s'exerce leur droit d'accès et de rectification aux informations les concernant.

C. La modification de la norme simplifiée n° 20 relative à la gestion du patrimoine immobilier à caractère social

Parallèlement à sa recommandation du 20 décembre 2001, la Commission a modifié la norme simplifiée relative à la gestion du patrimoine immobilier à caractère social afin de préciser que les enquêtes d'occupation sociale et les enquêtes relatives au supplément de loyer solidarité ne permettaient pas, dans le cadre des traitements d'informations déclarés à la CNIL en vertu de cette norme simplifiée, le recueil de l'information relative à la nationalité.

Par ailleurs, la Commission a autorisé, dans le cadre de cette norme, que les informations relatives aux demandeurs de logement soient conservées pendant cinq ans et non plus une année, à compter de la date de dépôt ou de renouvellement de la demande, une durée de conservation de cinq ans paraissant mieux adaptée aux exigences du logement social.

D. La consécration d'autres préconisations de la CNIL sur la nature des documents pouvant être demandés aux candidats locataires

La CNIL a été par ailleurs associée aux réunions de la Commission nationale de concertation mise en place par le secrétariat d'État au Logement qui réunissait les organisations de bailleurs et de locataires afin de déterminer les documents exigés des candidats locataires.

La CNIL a rappelé qu'elle considérait comme excessive, au regard des dispositions générales de la loi « informatique et libertés », la demande de relevés bancaires, d'attestations « de bonne tenue du compte », de la carte d'assuré social ainsi que de la photographie d'identité dont on voit mal la pertinence en matière d'attribution d'un logement.

Ces préconisations sont désormais consacrées par l'article 162 de la loi dite « de modernisation sociale » du 17 janvier 2002 qui intègre dans son chapitre NI intitulé « Lutte contre les discriminations dans la location des logements » des dispositions nouvelles modifiant la loi n° 89-462 du 6 juillet 1989 tendant à améliorer les rapports locatifs et portant elle-même modification de la loi n° 86-1290 du 23 décembre 1986.

« En préalable à l'établissement du contrat de location, le bailleur ne peut demander au candidat à la location de produire les documents suivants :
photographie d'identité ;
carte d'assuré social ;
copie de relevé de compte bancaire ou postal ;
attestation de bonne tenue de compte bancaire ou postal ».

Telle est désormais la loi.

III. LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

La CNIL avait entrepris dès 2000 une étude d'ensemble sur la question de la cybersurveillance sur les lieux de travail dans le souci de suggérer aux entreprises et aux salariés utilisateurs l'adoption d'une règle du jeu équilibrée, comme elle l'a fait en matière de badges d'accès, d'autocommutateurs téléphoniques, de vidéosurveillance, etc.

Cette étude était motivée par l'aspect novateur de ces techniques mais également par l'opacité, en tout cas pour le commun des utilisateurs, qui entoure les conditions de leur utilisation.

Après avoir consulté des experts informatiques et tout particulièrement des experts en réseau, ainsi que les organisations syndicales des salariés (CGT, CFDT, FO, CFTC et CGC) et patronales (MEDEF et CGPME), la CNIL a élaboré un rapport d'étude soumis à consultation publique autour des quatre questions dont elle était le plus fréquemment saisie.

1) En quoi les technologies en réseau seraient-elles de nature différente que les précédents outils mis en place dans les entreprises ?

2) Quelle est la part de la vie privée et des libertés individuelles garanties aux salariés qui sont liés à l'employeur par un contrat de travail qui est d'abord un lien de subordination ?

3) Quel usage à des fins privées d'outils mis à la disposition des salariés par leur employeur est-il admis ?

4) Y a-t-il des limites au contrôle et à la surveillance que les employeurs peu vent exercer sur les salariés ?

Cette concertation a donné lieu à un premier rapport d'étude et de consultation publique rendu public le 28 mars 2001 dans lequel la Commission a apporté un certain nombre de précisions *[cf.* 21^{e} rapport annuel, p. 121). Ce premier rapport, mis en ligne sur le site www.cnil.fr, a rencontré un large écho. Il a suscité diverses contributions de la part de groupes professionnels, de représentants syndicaux ou de particuliers, accessibles depuis le site de la CNIL.

Toutes les questions soulevées par la Commission ne relèvent évidemment pas de sa seule compétence. Mais, imbriquées les unes aux autres, elles constituent

un champ de préoccupations communes aux employeurs et aux salariés à l'heure de la société de l'information.

Parallèlement aux premières orientations ainsi esquissées par la CNIL, plusieurs de ses homologues européens adoptaient des recommandations en la matière. Tel était notamment le cas des commissaires à la protection des données britannique, belge et néerlandais.

A ce jour, le groupe européen des commissaires à la protection des données, institué par l'article 29 de la directive du 24 octobre 1995, a inscrit ce thème dans son programme de travail et rendra public un avis qui devrait témoigner de la forte convergence de vues entre autorités de protection des données des États membres de l'Union européenne.

À l'issue de ce premier travail d'approfondissement et de consultation, il revenait à la CNIL, pour ce qui la concerne, et compte tenu des nombreuses demandes de conseil, plaintes ou demandes de renseignements dont elle est saisie dans le cadre de ses missions, de faire part d'éclaircissements et de conclusions sur ce sujet.

C'est ainsi que la Commission a adopté le 5 février 2002 son rapport définitif sur le sujet de la cybersurveillance sur les lieux de travail.

A. Les lignes directrices

L'INFORMATION PRÉALABLE, CONDITION DE LA TRANSPARENCE

L'obligation d'information préalable résulte de l'article L. 121-8 du code du travail (« *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 l'emploi ».*

L'obligation de transparence inspire la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui soumet tout traitement automatisé d'informations nominatives à déclaration préalable auprès de la CNIL, interdit que les données soient collectées par un moyen frauduleux, déloyal ou illicite et impose une obligation d'information des personnes concernées notamment sur les destinataires des données et le lieu où s'exerce le droit d'accès et de rectification.

Qu'elle résulte des dispositions du code du travail ou de la loi du 6 janvier 1978, l'information préalable, condition de la loyauté de la collecte des données, est donc une condition nécessaire. Elle n'est pas suffisante.

LA DISCUSSION COLLECTIVE

L'article L. 432-2 du code du travail dispose que « *le comité d'entreprise est informé et consulté préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur […] les conditions de travail du personnel »* et précise que « *lorsque l'employeur envisage*

de mettre en œuvre des mutations technologiques importantes et rapides » le plan d'adaptation doit être transmis « *pour information et consultation »* au comité d'entreprise, lequel doit être *« régulièrement informé et périodiquement consulté »* sur la mise en œuvre de ce plan.

Par ailleurs, l'article L. 432-2-1 prescrit que le comité d'entreprise doit être « *informé et consulté, préalablement à la décision de mise en* œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ».

Le décret du 28 mai 1982 relatif aux comités techniques paritaires des trois fonctions publiques prévoit pour sa part que ces comités *« connaissent […] des questions et des projets de textes relatifs »,* notamment « aux *programmes de modernisation des méthodes et techniques du travail et à leur incidence sur la situation du personnel ».*

Il résulte clairement de ces textes, qu'une information individuelle des salariés ou agents publics ne saurait dispenser les responsables concernés de l'étape de la discussion collective, institutionnellement organisée, avec les représentants élus du personnel.

Compte tenu de ces textes, la CNIL vérifie, lorsqu'elle est saisie d'une demande d'avis ou d'une déclaration relative à un traitement automatisé d'informations nominatives mise en œuvre à des fins de contrôle, que ces consultations ont été effectuées préalablement à sa saisine, condition de régularité du projet de traitement déclaré à la Commission.

LA PROPORTIONNALITE

« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché ».

Ce principe désormais codifié sous l'article L. 120-2 du code du travail a été appliqué tant par les juridictions administratives que par les juridictions judiciaires, à l'occasion notamment des contentieux portant sur la régularité des règlements intérieurs. Les juridictions exercent un contrôle *a posteriori* des restrictions que l'employeur peut légalement apporter aux droits des personnes et aux libertés individuelles, la jurisprudence dessinant ainsi les contours d'une part sans doute résiduelle mais irréductible de liberté personnelle et de vie privée sur le lieu du travail.

« *Le salarié a droit, même au temps et au lieu de travail, au respect de sa vie privée ; celle-ci implique en particulier le secret de ses correspondances ; l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié ou reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».* C'est ce qu'a affirmé la chambre sociale de la Cour de Cassation dans un arrêt du 2 octobre 2001.

Le principe de protection de l'intimité de la vie privée du salarié sur son lieu de travail n'est pas nouveau et a été affirmé à des nombreuses reprises, notamment par la Cour européenne des Droits de l'Homme qui a fait application de l'article 8 de la Convention européenne de sauvegarde des Droits de l'Homme et des libertés fondamentales (« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ») dans les domaines relevant de la vie professionnelle — affaire *N. c/Allemagne* du 23 novembre 1992 et *H. C/Royaume-Uni* du 27 mai 1997.

Ce principe est cependant d'une application plus délicate à l'heure des nouvelles technologies qui laissent des « traces ». En effet, le phénomène de convergence ne permet plus de distinguer nettement ce qui relèverait de la vie professionnelle et ce qui ressortirait de l'intimité de la vie privée.

De manière générale, qu'il s'agisse d'assurer le bon fonctionnement du service informatique, la « sécurité numérique » de l'entreprise ou le confort de l'usager, ces « traces » sont intrinsèquement liées à la mise à disposition d'une telle technologie. Aussi, n'est-ce pas leur existence mais leur traitement à des fins autres que techniques qui doit être proportionné au but recherché.

Compte tenu du caractère évolutif des techniques et de la jurisprudence qui se dégage sur ces sujets, il convient de former les organisations et les utilisateurs sur les mesures de sécurité, de consultation ou d'information à prendre. De nombreuses entreprises ou administrations le font déjà.

Deux idées communément admises sont inexactes.

La première consiste à soutenir que l'ordinateur personnel mis à la disposition des utilisateurs sur leur lieu de travail serait, en tant que tel, protégé par la loi « informatique et libertés » et relèverait de la vie privée du salarié. Il n'en est rien : un ordinateur mis à la disposition d'un salarié ou d'un agent public dans le cadre de la relation de travail est la propriété de l'entreprise ou de l'administration et ne peut comporter que subsidiairement des informations relevant de l'intimité de la vie privée.

Il peut être protégé par un mot de passe et un « login », mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers ; elle n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé.

La deuxième idée consiste à prétendre qu'une information préalable des personnels suffirait. De nombreuses entreprises ou administrations imaginent qu'une information préalable des salariés suffirait à se prémunir de tout problème et à autoriser l'emploi de tous les modes de surveillance et de contrôle. Dans le souci de se garantir contre tout aléa, elles peuvent quelquefois être tentées de déclarer à la CNIL leur schéma de sécurité d'ensemble.

Une telle manière de procéder n'est pas suffisante dès lors que les finalités seraient mal définies ou mal comprises. En outre, elle peut nourrir, à tort, le sentiment des utilisateurs qu'ils se trouveraient sous un contrôle constant de l'organisation alors que les mesures prises, dans bien des cas, se bornent à assurer la sécurité du système

ou celle des applications et non pas un contrôle individuel ou nominatif de leur activité. Enfin, elle peut conforter l'entreprise ou l'administration dans l'idée qu'une déclaration à la CNIL de l'ensemble de son système de sécurité l'autoriserait à porter des atteintes à ce que commande le respect de l'intimité de la vie privée et de la liberté personnelle résiduelle du salarié sur son lieu de travail, alors qu'il appartient, en dernière instance, aux juridictions administratives ou judiciaires d'en apprécier la régularité et, compte tenu des circonstances de fait ou de droit de l'espèce, la proportionnalité.

B. Le contrôle des connexions à Internet

Une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication. Un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité paraît généralement et socialement admis par la plupart des entreprises ou administrations.

Aucune disposition légale n'interdit évidemment à l'employeur d'en fixer les conditions et limites, lesquelles ne constituent pas, en soi, des atteintes à la vie privée des salariés ou agents publics.

À ce titre, la mise en place de dispositifs de filtrage de sites non autorisés, associés au pare-feu (sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionnistes etc.) peut constituer une mesure de prévention dont il y a lieu d'informer les salariés ou agents publics.

De même, la possibilité pour les salariés ou agents publics de se connecter à Internet à des fins autres que professionnelles peut s'accompagner de prescriptions légitimes dictées par l'exigence de sécurité de l'entreprise, telles que l'interdiction de télécharger des logiciels, l'interdiction de se connecter à un forum ou d'utiliser le « chat », l'interdiction d'accéder à une boîte aux lettres personnelle par Internet compte tenu des risques de virus qu'un tel accès est susceptible de présenter.

Un contrôle a *posteriori* des données de connexion à Internet, de façon globale, par service ou par utilisateur ou un contrôle statistique des sites les plus visités devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle nominatif individualisé des sites accédés.

Les modalités d'un tel contrôle de l'usage d'Internet doivent, conformément à l'article L. 432-2-1 du code du travail, faire l'objet d'une consultation du comité d'entreprise ou, dans la fonction publique, du comité technique paritaire ou de toute instance équivalente et d'une information des utilisateurs, y compris lorsque le contrôle est dépourvu d'un caractère directement nominatif.

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel destiné à produire, poste par poste, un relevé des durées de connexion ou des sites visités, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la CNIL. La durée pendant laquelle les relevés ainsi établis sont conservés doit être précisée. Une durée de conservation de l'ordre de six mois

devrait être suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'Internet.

C. Le contrôle de l'usage de la messagerie

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, un message à caractère personnel correspond à un usage généralement et socialement admis. D'ailleurs, compte tenu des termes de l'arrêt de la chambre sociale de la Cour de Cassation en date du 2 octobre 2001 une interdiction ne permettrait pas à l'employeur de prendre connaissance dans des conditions régulières du contenu de celles des correspondances qui relèveraient de la vie privée des personnes.

Il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste du travail mis à disposition par l'entreprise ou l'administration revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire qui lui conférerait alors le caractère et la nature d'une correspondance privée, protégée par le secret des correspondances.

Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises ou les administrations à mettre en place des outils de mesure de la fréquence ou de la taille des fichiers transmis en pièce jointe au message électronique ou encore des outils d'archivage des messages échangés. Dans cette dernière hypothèse, le message électronique bien qu'étant effacé du poste de l'émetteur et du poste du récepteur sera néanmoins conservé. L'emploi de tels outils de contrôle ou de sauvegarde doit être porté à la connaissance des salariés ainsi que la durée de conservation du message « sauvegardé ».

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la CNIL. La durée pendant laquelle les messages sont conservés doit être précisée.

D. Les fichiers de journalisation

Les fichiers de journalisation des connexions destinés à identifier et enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations constituent une mesure de sécurité, généralement préconisée par la CNIL dans le souci que soient assurées la sécurité et la confidentialité des données à caractère personnel, lesquelles ne doivent pas être accessibles à des tiers non autorisés, ni utilisées à des fins étrangères à celles qui justifient leur traitement. Ils n'ont pas pour vocation première le contrôle des utilisateurs.

La finalité de ces fichiers de journalisation qui peuvent également être associés à des traitements d'informations dépourvus de tout caractère nominatif mais revêtent un caractère sensible pour l'entreprise ou l'administration concernée

consiste à garantir une utilisation normale des ressources des systèmes d'information et, le cas échéant, à identifier les usages contraires aux règles de confidentialité ou de sécurité des données définies par l'entreprise.

Ces fichiers de journalisation lorsqu'ils sont associés à un traitement automatisé d'informations nominatives n'ont pas, en tant que tels, à faire l'objet des formalités préalables auprès de la CNIL. Afin de garantir ou de renforcer l'obligation de sécurité, ils doivent être portés à la connaissance de la CNIL au titre des mesures de sécurités entourant le fonctionnement du traitement principal dont ils sont le corollaire.

En revanche, la mise en oeuvre d'un logiciel d'analyse des différents journaux (applicatifs et systèmes) permettant de collecter des informations individuelles poste par poste destiné à contrôler l'activité des utilisateurs, doit être déclarée à la CNIL.

Dans tous les cas de figure, les utilisateurs doivent être informés de la mise en place des systèmes de journalisation et de la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur s'étant connecté sont conservées ou sauvegardées. Cette information qui réalise l'obligation légale à laquelle est tenue le responsable du traitement est de nature à prévenir tout risque et participe de l'exigence de loyauté dans l'entreprise ou l'administration.

Une durée de conservation de l'ordre de six mois ne paraît pas excessive au regard de la finalité des fichiers de journalisation.

Aucune disposition de la loi du 6 janvier 1978 ne prive le responsable de l'entreprise de la possibilité d'opposer les informations enregistrées dans les fichiers de journalisation associés à un traitement automatisé d'informations nominatives à un salarié ou un agent public qui n'en n'aurait pas respecté les conditions d'accès ou d'usage (Cour de Cassation B chambre sociale n° 98-43 485 du 18 juillet 2000).

E. Le rôle des administrateurs de réseaux

Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits, par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à Internet, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978.

De même, l'utilisation encadrée de logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou à prendre le contrôle, à distance, du poste de travail d'un salarié (« prise de main à distance ») ne soulève aucune difficulté particulière au regard de la loi du 6 janvier 1978 à condition que les mesures de sécurité nécessaires à la protection des données soient mises en œuvre.

Toutefois, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont les administrateurs

de réseaux et systèmes peuvent avoir connaissance dans l'exercice de leurs fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique.

De même, les administrateurs de réseaux et systèmes, tenus au secret professionnel, ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

F. Sécurité renforcée en cas d'utilisation des technologies de l'information et de la communication par les instances représentatives du personnel

Les entreprises et administrations négocient quelquefois les conditions dans lesquelles la messagerie de l'entreprise peut être utilisée par les instances représentatives du personnel ou pour l'exercice d'un mandat syndical.

Lorsque les instances représentatives du personnel disposent d'un compte de messagerie dédié, des mesures de sécurité particulières devraient être définies ou mises en œuvre afin d'assurer la confidentialité des informations échangées.

Les modalités d'utilisation des technologies de l'information et de la communication de l'entreprise par les représentants syndicaux pour exercer leur mandat devraient également être précisées.

G. Deux propositions concrètes

UN BILAN ANNUEL « INFORMATIQUE ET LIBERTÉS »

La Commission estime que les mesures de sécurité qui conduisent à conserver trace de l'activité des utilisateurs ou de l'usage qu'ils font des technologies de l'information et de la communication ou qui reposent sur la mise en œuvre de traitements automatisés d'informations directement ou indirectement nominatives devraient faire l'objet d'un bilan annuel « informatique et libertés » à l'occasion de la discussion du bilan social soumis au comité d'entreprise ou au comité technique paritaire ou à toute autre instance équivalente. En tout état de cause, des initiatives de ce type seraient de nature à préserver la confiance de l'entreprise ou de l'administration à l'égard des nouvelles technologies.

LA DÉSIGNATION D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Dans le même esprit, la Commission souhaite que les entreprises ou les administrations pourraient désigner, dès lors que leurs effectifs et leur mode d'organisa-

tion le justifieraient et le leur permettraient, en concertation avec les instances représentatives du personnel, un « délégué à la protection des données et à l'usage des nouvelles technologies dans l'entreprise ». Ce délégué pourrait être plus particulièrement chargé des questions relevant des mesures de sécurité, du droit d'accès et de la protection des données personnelles sur le lieu de travail. Interlocuteur des responsables de l'entreprise ou de l'administration ainsi que des instances représentatives du personnel et des salariés ou agents publics, ce délégué pourrait devenir un « correspondant informatique et libertés » dans l'entreprise sur ces questions.

IV. UN SYSTEME NATIONAL D'INFORMATION SUR LES DÉPENSES DE SANTÉ : LE SNIIRAM

Dans le domaine social comme dans d'autres secteurs, la CNIL constate depuis plusieurs années une tendance marquée à la centralisation des informations et à la constitution de bases de données nationales.

La statistique et le contrôle sont les raisons généralement invoquées, plus ou moins explicitement, pour justifier la création de ces fichiers centraux, de ces « entrepôts de données ». Pour un gestionnaire, il peut en effet paraître plus aisé de disposer d'informations rassemblées dans une base unique, et immédiatement exploitables grâce aux outils de requêtes sophistiqués[1] que de devoir procéder par exploitation de fichiers locaux.

Confrontée à ces projets, parfois fort ambitieux et qui résultent le plus souvent de dispositions législatives, la CNIL s'efforce de mener, en liaison avec les acteurs concernés, une réflexion sur les implications d'un tel recueil exhaustif et un travail d'analyse sur l'utilité de disposer, au regard de l'objectif poursuivi, de telle ou telle donnée.

A. Une base de données exhaustive

Ainsi en est-il du SNIIRAM, système national d'information interrégimes, qui a été institué par la loi de financement de la sécurité sociale pour 1999 (article L. 161-28-1 du code de la Sécurité sociale) dans le souci de permettre une meilleure connaissance des dépenses de l'ensemble des régimes d'assurance maladie moyennant une contrepartie : transmettre, en retour, aux prestataires de soins des informations relatives à leur activité, leurs recettes et s'il y a lieu à leurs prescriptions.

[1] Recourant aux techniques de « *datawarehouse* » et de « *datamining* » ; ces techniques permettent à des utilisateurs d'effectuer facilement exploitations, tris, mises en relation d'informations et de lancer des requêtes complexes sur des quantités de données qui sont stockées dans des « entrepôts de données ».

Cette base de données, gérée par le centre national de traitement informatique de la CNAMTS, a vocation à comporter l'ensemble des données issues des fichiers des caisses, quel que soit le régime de sécurité sociale concerné. Les informations ainsi rassemblées en une base unique résultent *du* traitement des feuilles de soins (y compris les données du codage des actes, des prestations et à terme des pathologies) et des prescriptions, et, s'agissant des données relatives à l'activité hospitalière, du Programme de médicalisation des systèmes d'information (PMSI), système d'information constitué à partir des données d'activité fournies par les établissements de santé.

Pour les pouvoirs publics, la création du SNIIRAM est justifiée par la nécessité d'améliorer la connaissance des statistiques de l'assurance maladie. En effet, les systèmes d'information existants, soit qu'ils soient propres à chaque régime, soit qu'ils soient parcellaires car reposant sur de simples accords entre régimes, ne permettent pas de disposer de statistiques fiables et complètes, dont la connaissance est utile au Parlement pour se prononcer sur l'évolution de l'ensemble des dépenses de l'assurance maladie, à travers l'Objectif national des dépenses de l'assurance maladie (ONDAM).

Par ailleurs, la politique de maîtrise médicalisée de l'évolution des dépenses de santé, initiée en 1993 avec la mise en place du codage détaillé des actes, des prestations et des pathologies, a conduit les pouvoirs publics à prévoir, dans le souci de faciliter l'adhésion des professionnels de santé concernés au dispositif dans son ensemble, un retour d'informations destiné à les convaincre de l'utilité de ce système d'information.

Les catégories d'informations concernent l'identification des organismes de prise en charge, les caractéristiques des décomptes de remboursement, les numéros d'anonymat des assurés et des bénéficiaires, le sexe, l'année et le mois de naissance, le département et la commune de résidence, les informations relatives aux prestations servies, comportant notamment le code détaillé des actes, biens et services présentés au remboursement ainsi que le code des pathologies, le numéro d'identification des professionnels de santé, le sexe, la date de naissance, la spécialité médicale, la nature d'exercice, le statut conventionnel, la caisse de rattachement, le département et la commune d'établissement, les informations relatives à l'activité des établissements de santé et des données comptables.

Le SNIIRAM doit être accessible à l'ensemble des caisses des différents régimes de base et des caisses nationales, aux Unions régionales des caisses d'assurance maladie (URCAM), aux Agences régionales d'hospitalisation, aux Unions régionales des médecins libéraux (URML), au ministère de l'Emploi et de la Solidarité et au ministère de l'Agriculture et bien entendu aux prestataires de soins pour les données concernant leur activité. Il n'est pas exclu, à terme et dès lors que la CNIL l'aurait autorisé dans les conditions prévues au chapitre V *ter* de la loi *du 6* janvier 1978, qu'elles soient communiquées à d'autres partenaires, tels que les assureurs complémentaires.

Les informations concernant les professionnels de santé figureront dans la base sous forme nominative puisque le SNIIRAM doit permettre un retour

d'informations à chacun d'entre eux sur son activité. En revanche, la base de données ne peut comporter aucune donnée nominative sur les bénéficiaires de soins, la loi disposant expressément que « les données reçues et traitées par le système national d'information interrégimes de l'assurance maladie préservent l'anonymat des personnes ayant bénéficié des prestations de soins ».

La loi a également prévu que les modalités de gestion de cette base de données, définies conjointement par protocole passé au moins entre la CNAMTS, la MSA et la CANAM, doivent être approuvées par un arrêté du ministre chargé de la Sécurité sociale, pris après avis motivé de la CNIL.

B. Les conditions imposées par la CNIL

Compte tenu de l'ampleur du dispositif projeté, en particulier de la sensibilité des informations appelées à figurer dans le SNIIRAM et de leur exhaustivité, des modalités d'exploitation de celles-ci et du grand nombre d'utilisateurs susceptibles d'avoir accès à la base, la Commission a mené, pendant près de deux ans, une concertation approfondie avec le ministère et la CNAMTS, maître d'œuvre du SNIIRAM afin que toutes précautions soient prises pour assurer de façon effective l'anonymat et la sécurité des données. La CNIL a ainsi obtenu sur plusieurs points des modifications substantielles du projet. Après avoir procédé à l'audition du directeur de la Sécurité sociale, du directeur des exploitations, de la politique sociale et de l'emploi (ministère de l'Agriculture) ainsi que des directeurs de la CNAMTS et de la Caisse centrale de mutualité sociale agricole, elle a finalement rendu le 18 octobre 2001 un avis favorable sur le projet qui lui était présenté, tout en formulant un certain nombre de réserves et de demandes.

Tout en observant que les finalités poursuivies par le SNIIRAM étaient parfaitement légitimes, la CNIL a cependant souhaité obtenir des précisions sur un certain nombre de points tenant en particulier aux conditions d'utilisation des données et aux mesures de sécurité.

Il a ainsi été demandé à la CNAMTS de définir plus précisément les types de traitements statistiques susceptibles d'être effectués. Une liste de treize thèmes d'analyse de l'offre de soins a donc été établie, liste dont la Commission a souhaité qu'elle soit validée par le conseil pour la transparence des statistiques de l'assurance maladie qui est chargé, en application du code de la sécurité sociale, d'une mission d'expertise sur la nature et les destinataires des productions statistiques utiles à la connaissance des pratiques de soins de ville et des dépenses de santé. La Commission avait bien sûr pris acte que les professionnels de santé seraient associés à la mise en œuvre du SNIIRAM dans la mesure où leurs représentants sont membres de droit de ce conseil et où ils seront invités à participer, par le biais de leurs instances représentatives, au comité d'orientation et de pilotage du SNIIRAM.

1 — LA GARANTIE DE L'ANONYMAT DES PATIENTS

Les noms, prénoms, numéros de sécurité sociale, adresses des bénéficiaires de soins ne seront pas transmis au SNIIRAM et ne figurent pas dans la base nationale de données.

Mais au-delà de cette première garantie — essentielle —, il est apparu nécessaire, de définir des dispositifs qui garantissent non seulement que des données directement ou indirectement nominatives sur les assurés ne puissent être transmises mais également que les données figurant dans la base ne puissent permettre l'identification des assurés par recoupement d'informations. Ces dispositifs de sécurité, développés par le centre d'études des sécurités du système d'information (CESSI) de la CNAMTS ont fait l'objet de plusieurs réunions de travail techniques avec les services de la CNIL

Il sera ainsi procédé, avant toute transmission des données, au « transcodage » irréversible de tous les matricules identifiants (NIR de l'assuré et du bénéficiaire, identifiants de la pension d'invalidité, de la rente d'accident du travail ou de maladie professionnelle, numéro d'entrée du patient dans l'établissement de santé) en des numéros non signifiants qui permettront sans réidentification possible de la personne concernée, d'apparier, de « chaîner » les données relatives aux différentes prestations qui lui ont été servies. De surcroît, lors de la réception par la CNAMTS de ces numéros dits « d'anonymisation », il sera à nouveau procédé à une deuxième opération de « transcodage » afin que les numéros permettant d'apparier des informations relatives à une même personne soient différents des numéros d'anonymisation créés par les caisses et utilisés lors de la transmission.

Cette technique de double anonymisation, préconisée par la CNIL dans les cas les plus sensibles et évaluée, à la demande de la Commission en 1996 et 1997 par le service central de la sécurité des systèmes d'information, est déjà utilisée pour la transmission, par les cliniques, d'informations sur leur activité (PMSI privé), pour certaines recherches épidémiologiques et enquêtes dans le domaine social (observatoire du RMI à Paris), et doit être employée pour le système de surveillance des cas de séropositivité ainsi que pour le « chaînage » des séjours dans le cadre du PMSI public.

Par ailleurs, afin de prévenir tout risque de réidentification d'une personne par recoupement de plusieurs informations, certaines recherches croisées à partir de variables potentiellement identifiantes (mois de naissance associé au code commune de résidence, code affiné de la prestation, discipline de prestation, code affection longue durée (ALD) et pathologies associées, jour des soins, code pathologie) seront interdites.

Enfin, un logiciel de filtrage permettra de recenser toute requête dont le dénombrement des bénéficiaires concernés serait inférieur ou égal à dix, interdisant dans cette hypothèse, l'affichage à l'écran ou l'édition des résultats issus de telles requêtes.

2 — DES RÈGLES RIGOUREUSES DE SECURITE ET D'AUTORISATION D'ACCÈS

Outre ces dispositifs d'anonymisation, des procédures de sécurité seront mises en œuvre pour assurer, lors de la transmission des données entre les différents partenaires, leur authentification réciproque par un dispositif de signature électronique, l'intégrité des données (par un mécanisme de scellement recourant aux techniques cryptographiques), la confidentialité des informations (par des procédures de chiffrement fort), et enfin le contrôle des opérations effectuées (par la conservation d'un historique des échanges).

Une journalisation des interrogations sera mise en oeuvre et l'exploitation systématique de celle-ci réalisée.

Enfin, il sera procédé au chiffrement des fichiers de sauvegarde.

Compte tenu du nombre important d'utilisateurs prévus, la Commission a estimé que les autorisations d'accès devaient être précisément définies, s'agissant en particulier, des personnels habilités à y avoir accès et des catégories de données susceptibles d'être accessibles.

Les règles d'autorisation d'accès qui ont été établies reposent sur les principes suivants.

1) Seuls les médecins conseils des échelons locaux et régionaux des services médicaux des caisses, les personnels placés sous leur responsabilité ainsi que les agents administratifs des caisses et des URCAM, ceux-ci nommément désignés par les directeurs ou agents comptables de ces organismes[1] , seront habilités à avoir accès à l'ensemble des données figurant dans le SNIIRAM, c'est-à-dire aux données individuelles mais anonymisées concernant les bénéficiaires de soins et aux données en clair concernant les professionnels de santé. Toutefois, seuls les médecins conseils seront habilités à effectuer certaines recherches croisées sur des variables potentiellement identifiantes (code commune, date des soins, mois et année de naissance) et les utilisateurs selon leurs fonctions, pourront n'avoir accès, au sein de la base nationale, qu'à des informations concernant leur région.

2) Les unions régionales des médecins libéraux, les agences régionales d'hospitalisation, les DDASS et le ministère de l'Emploi et de la Solidarité et le ministère de l'Agriculture n'auront accès aux données que sous la forme de statistiques agrégées. Ni l'identification en clair des professionnels des santé ni les données individuelles relatives aux bénéficiaires de soins ne leur seront accessibles.

3) Les professionnels de santé auront accès aux données relatives à leur activité, leurs recettes ou leurs prescriptions et donc aux données individuelles « anonymisées » concernant leurs patients.

Au plan technique, une grille d'habilitation et quatorze profils de droits ont ainsi été définis.

[1] soit en moyenne cinq personnes par caisse locale.

Au sein des organismes et administrations, les personnels autorisés à accéder aux données devront être nommément désignés par les directeurs ou agents comptables concernés, selon des règles précises : ainsi un utilisateur ne sera habilité à accéder au SNIIRAM que s'il a été identifié et authentifié par une carte de sécurité ou un mot de passe et s'il est présent sur un annuaire géré par la CNAMTS qui précisera le profil auquel il est habilité et les dates de début et de fin de validité de cette autorisation.

3 — L'INFORMATION DES PROFESSIONNELS DE SANTE

Compte tenu des finalités poursuivies, il est apparu que les professionnels de santé devaient être clairement informés des modalités de mise en oeuvre du SNIIRAM.

La CNAMTS s'est ainsi engagée à informer individuellement par courrier les professionnels de santé des modalités de mise en oeuvre du SNIIRAM et des conditions d'exercice de leur droit d'accès et de rectification auprès de la caisse de leur circonscription ou de rattachement. À cet égard, la communication systématique aux professionnels de santé des informations concernant leur activité, est de nature à garantir que ces droits pourront ainsi être pleinement exercés.

Délibération n° 01-054 du 18 octobre 2001 portant avis sur le projet d'arrêté présenté par le ministère de l'Emploi et de la Solidarité relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie (SNIIRAM)

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu l'article L. 161-28-1 du code de la Sécurité sociale ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le projet d'arrêté présenté par la ministre de l'Emploi et de la Solidarité ;

Vu le protocole et ses annexes, transmis par la ministre de l'Emploi et de la Solidarité définissant les modalités de gestion et de renseignement du SNIIRAM, le contenu des données, la charte d'utilisation, les missions et les modalités de fonctionnement de la commission d'habilitation, chargée d'assurer la sécurisation des accès au SNIIRAM, le plan qualité qui doit garantir un traitement homogène des données, la composition et les modalités d'organisation du . comité d'orientation et de pilotage chargé de sa mise en œuvre ;

Après avoir procédé, le 9 octobre 2001, à l'audition du directeur de la Sécurité sociale du ministère de l'Emploi et de la Solidarité, du directeur des exploitations, de la politique sociale et de l'emploi au ministère de l'Agriculture, du directeur de la CNAMTS, du médecin conseil national placé auprès de la CNAMTS, et du directeur de la CCMSA ;

Après avoir entendu Monsieur Maurice Viennois en son rapport et Madame Charlotte-Marie Pitrat, Commissaire du Gouvernement en ses observations ;

Saisie pour avis, par le ministère de l'Emploi et de la Solidarité d'un projet d'arrêté relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie (SNIIRAM) ;

Formule les observations suivantes :

Créé par l'article 21 de la loi 98-1194 du 23 décembre 1998 de financement de la Sécurité sociale pour 1999 (article L. 161-28-1 du code de la Sécurité sociale), le système national d'information interrégimes de l'assurance maladie (SNIIRAM) a pour objet de contribuer :
1) « à la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépenses, par catégories de professionnels responsables de ces dépenses et par professionnel ou établissement ;
2) à la transmission en retour aux prestataires de soins d'informations pertinentes relatives à leur activité, leurs recettes et s'il y a lieu à leurs prescriptions ».

Aux termes de cet article, les modalités de gestion et de renseignement du système national sont définies conjointement par protocole passé au moins entre la CNAMTS, la MSA et la CANAM et doivent être approuvées par un arrêté du ministre chargé de la Sécurité sociale, pris après avis motivé de la CNIL, cet arrêté tenant lieu d'acte réglementaire des organismes d'assurance maladie, au sens de l'article 15 de la loi du 6 janvier 1978.

La Commission relève que ce système national d'information, qui sera constitué d'une seule base de données, gérée par le Centre national de traitement informatique (CENTI) de la CNAMTS, a vocation à comporter les données issues des fichiers des caisses gérant un régime de base de l'assurance maladie et en particulier les informations résultant du traitement des feuilles de soins, y compris les données du codage des actes, des prestations et à terme des pathologies, et des prescriptions, ainsi que les données sur l'activité hospitalière, issues du Programme de médicalisation des systèmes d'information (PMSI), système d'information constitué à partir des données d'activité fournies par les établissements de santé.

Elle observe cependant que le SNIIRAM ne doit pas comporter de données nominatives sur les bénéficiaires de soins, la loi disposant expressément que « les données reçues et traitées par le système national d'information interrégimes de l'assurance maladie préservent l'anonymat des personnes ayant bénéficié des prestations de soins ». En revanche les données relatives aux professionnels de santé enregistrées dans le SNIIRAM comporteront leur numéro d'identification professionnelle.

Il revient en conséquence à la Commission de s'assurer que les modalités de fonctionnement du SNIIRAM respectent les objectifs et contraintes fixés par le législateur ainsi que les dispositions de la loi du 6 janvier 1978.

Sur les finalités du SNIIRAM

Aux termes de l'article 2 du projet d'arrêté, les traitements mis en œuvre dans le cadre du SNIIRAM ont pour finalités :
1) d'améliorer la qualité des soins, notamment par la comparaison des pratiques aux référentiels, au sens de l'article L 162-12-15 du code de la sécurité sociale, et moyennes professionnelles ;
2) de contribuer à une meilleure gestion de l'assurance maladie, notamment par :
— la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépenses, par ca tégories de professionnels responsables de ces dépenses et par profession nel ou établissement ;
— l'évaluation des transferts entre enveloppes correspondant aux objectifs sectoriels de dépenses fixés, en fonction de l'objectif national de dépenses d'assurance maladie, dans le cadre de la loi annuelle de financement de la sécurité sociale ;
— l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;
3) d'assurer la transmission aux prestataires de soins d'informations pertinen tes relatives à leur activité, leurs recettes et, s'il y a lieu, à leurs prescriptions.
Ces finalités ont conduit les caisses nationales de sécurité sociale à définir treize thèmes d'analyse de l'offre de soins, énumérés en annexe de la pré sente délibération.

La Commission en prend acte mais estime que cette liste devra être validée en accord avec le conseil pour la transparence des statistiques de l'assurance maladie, chargé, aux termes de l'article L. 161-28-3 du code de la Sécurité sociale, de contribuer par ses avis à définir la nature et les destinataires des productions statistiques dans le domaine de soins de ville, utiles à la connaissance des pratiques de soins et des dépenses de santé. La Commission observe que les finalités poursuivies sont légitimes dans la mesure où elles doivent permettre, dans le cadre des objectifs fixés par le législateur, d'améliorer la connaissance statistique des dépenses de l'assurance maladie et du fonctionnement du système de soins, s'agissant tout particulièrement des caractéristiques de l'évolution de l'offre de soins. Elle prend acte de ce que les professionnels de santé seront associés à la mise en œuvre du SNIIRAM dans la mesure où d'une part, conformément au protocole, ils seront invités à participer, par le biais de leurs instances représentatives, au comité d'orientation et de pilotage du système d'information interrégimes et où, d'autre part, en application de l'article L. 161-28-2 du code de la Sécurité sociale, les représentants des professionnels de santé sont membres de droit du conseil pour la transparence des statistiques de l'assurance maladie.

Sur les catégories de personnes concernées

dispositions prises pour garantir l'anonymat des bénéficiaires de soins

La Commission prend acte de ce que :
— les noms, prénoms, numéros de sécurité sociale, adresses des bénéficiai res de soins ne seront pas transmis au SNIIRAM et ne figurent pas dans la base nationale de données ;

— il sera en outre procédé, avant toute transmission des données, à l'« ano nymisation » de tous les matricules identifiants (NIR de l'assuré et du bénéfi ciaire, identifiants de la pension d'invalidité, de la rente d'accident du travail ou de maladie professionnelle, numéro d'entrée du patient dans l'éta blissement de santé) c'est-à-dire au « transcodage » de ces matricules, selon un dispositif de codage irréversible, en des numéros non signifiants qui per mettront sans réidentification possible de la personne concernée, d'apparier les données relatives aux différentes prestations qui lui ont été servies. De surcroît, lors de la réception à la CNAMTS de ces numéros d'anonymisation, il sera à nouveau procédé à une deuxième opération de « transcodage » afin que les numéros permettant dans la base nationale d'apparier des infor mations relatives à une même personne soient différents des numéros d'ano nymisation créés par les caisses et utilisés lors de la transmission ;

— afin de prévenir tout risque de réidentification d'une personne par recou pement de plusieurs informations, seront interdites certaines recherches croi sées à partir de variables potentiellement identifiantes (mois de naissance et code commune de résidence, code affiné de la prestation, discipline de pres tation, code affection longue durée (ALD) et pathologies associées, jour des soins, code pathologie) ;

— un logiciel de filtrage permettra de recenser toute requête dont le dénom brement des bénéficiaires concernés sera inférieur ou égal à dix, et d'inter dire l'affichage à l'écran ou l'édition des résultats issus de telles requêtes.

La Commission considère que eu égard à la finalité statistique assignée par la loi au dispositif, à la sensibilité des informations appelées à figurer dans le SNIIRAM et aux modalités d'exploitation de celles-ci, la mise en œuvre de l'ensemble de ces mesures est nécessaire et adaptée pour garantir de façon satisfaisante l'anonymat des données concernant les bénéficiaires de soins.

Le caractère indirectement nominatif des informations relatives aux professionnels de santé

Dans la mesure où l'un des objectifs assignés au SNIIRAM par le législateur est la connaissance des dépenses d'assurance maladie par catégorie de professionnels de santé responsables de ces dépenses et par professionnel de santé ou établissement et qu'il est également prévu un retour d'informations à chaque professionnel concerné sur son activité, il est pertinent d'enregistrer, les informations les concernant, sous leur numéro d'identification professionnelle.

La Commission estime à cet égard que la communication systématique aux professionnels de santé des informations concernant leur activité, est de nature à garantir que les droits d'accès et de rectification qui leurs sont reconnus en application des articles 34 et suivants de la loi du 6 janvier 1978, pourront ainsi être pleinement exercés.

Sur les catégories d'informations

L'article L. 161-28-1 du code de la Sécurité sociale en son deuxième alinéa, précise que les organismes gérant un régime de base d'assurance maladie transmettent au SNIIRAM les données nécessaires.

Le projet d'arrêté soumis à la CNIL énumère de façon limitative, en son article 3, les catégories d'informations qui sont appelées à figurer dans le SNIIRAM et qui sont détaillées dans un tableau annexé au protocole.

Ces catégories d'informations concernent l'identification des organismes de prise en charge, les caractéristiques des décomptes de remboursement, les numéros d'anonymat des assurés et des bénéficiaires, le sexe, l'année et le mois de naissance, le département et la commune de résidence, les informations relatives aux prestations servies, comportant notamment le code détaillé des actes, biens et services présentés au remboursement ainsi que le code des pathologies, le numéro d'identification des professionnels de santé, le sexe, la date de naissance, la spécialité médicale, la nature d'exercice, le statut conventionnel, la caisse de rattachement, le département et la commune d'établissement, les informations relatives à l'activité des établissements de santé et des données comptables.

La Commission considère que ces catégories d'informations sont pertinentes au regard des finalités poursuivies mais estime nécessaire que le conseil pour la transparence des statistiques de l'assurance maladie soit consulté sur l'adéquation précise des informations aux thèmes d'analyse définis.

Sur les destinataires

Le projet d'arrêté énumère en son article 4 les destinataires susceptibles d'avoir accès au SNIIRAM et définit les règles d'autorisation d'accès. Ces règles reposent sur les principes suivants :

— seuls les médecins conseils des échelons locaux et régionaux des services médicaux des caisses, les personnels placés sous leur responsabilité ainsi que les agents administratifs des caisses et des URCAM, nommément désignés par les directeurs ou agents comptables de ces organismes, seront habilités à avoir accès à l'ensemble des données figurant dans le SNIIRAM, c'est-à-dire aux données individuelles mais anonymisées concernant les bénéficiaires de soins et aux données en clair concernant les professionnels de santé ;

— les unions régionales des médecins libéraux, les agences régionales d'hospitalisation, le ministère de l'Emploi et de la Solidarité, le ministère de l'Economie, des Finances et de l'Industrie et le ministère de l'Agriculture n'auront accès aux données que sous la forme de statistiques agrégées. Ni l'identification en clair des professionnels de santé ni les données individuelles relatives aux bénéficiaires de soins ne leur seront accessibles ;

— chaque professionnel de santé aura accès, pour ce qui le concerne, aux données relatives à son activité, ses recettes ou ses prescriptions.

La Commission prend acte de ce que, au sein des organismes et administrations concernés, les personnels autorisés à accéder aux données devront être nommément désignés à cet effet par les directeurs ou agents comptables concernés, selon des règles précises : ainsi un utilisateur ne sera habilité à accéder au SNIIRAM que s'il a été identifié et authentifié par une carte de sécurité ou un mot de passe et s'il est présent sur un annuaire géré par la CNAMTS qui précisera le profil auquel il est habilité et les dates de début et de fin de validité de cette autorisation.

La Commission observe qu'aux termes de l'article L. 161-28-4 du code de la Sécurité sociale, les organismes d'assurance maladie doivent communiquer au conseil pour la transparence des statistiques de l'assurance maladie les informations statistiques qu'ils produisent dans le domaine des soins de ville. Elle estime en conséquence que l'article 4 du projet d'arrêté doit être complété pour mentionner le Conseil au titre des destinataires des informations statistiques issues du SNIIRAM.

Sur les mesures de sécurité

La Commission prend acte de ce que, outre les dispositifs d'anonymisation adoptés :
— une journalisation des interrogations sera mise en œuvre et l'exploitation systématique de celle-ci réalisée ;
— des procédures de sécurité seront mises en oeuvre pour assurer, lors de la transmission des données entre les différents partenaires, leur authentification réciproque par un dispositif de signature électronique, l'intégrité des données (par un mécanisme de scellement recourant aux techniques cryptographiques), la confidentialité des informations (par des procédures de chiffrement fort), et enfin le contrôle des opérations effectuées (par la conservation d'un historique des échanges) ;
— enfin, il sera procédé au chiffrement des fichiers de sauvegarde.

La Commission considère que ces mesures sont de nature à assurer de façon convenable la confidentialité des informations.

Sur la durée de conservation

La Commission relève que les informations individuelles relatives aux bénéficiaires de soins seront conservées pendant deux ans au-delà de l'année en cours et que les données concernant les professionnels de santé dix ans.

Sur l'information des professionnels de santé

Compte tenu des finalités poursuivies, la Commission estime que les professionnels de santé doivent être clairement informés des modalités de mise en oeuvre du SNIIRAM.

La Commission prend acte à cet égard de l'engagement pris par la CNAMTS d'informer individuellement par courrier les professionnels de santé des modalités de mise en œuvre du SNIIRAM et des conditions d'exercice de leur droit d'accès et de rectification auprès de la caisse de leur circonscription ou de rattachement.

Émet, au bénéfice des observations qui précèdent, un avis favorable au projet d'arrêté présenté par le ministre de l'Emploi et de la Solidarité relatif à la mise en œuvre du système national d'information interrégimes d'assurance maladie, sous réserve que :
— la liste des thèmes d'analyse soit validée par le conseil pour la transparence des statistiques de l'assurance maladie[1];
— le conseil pour la transparence des statistiques de l'assurance maladie soit consulté sur l'adéquation précise des informations aux thèmes d'analyse définis ;
— l'article 4 du projet d'arrêté soit complété pour mentionner le conseil au titre des destinataires des informations statistiques issues du SNIIRAM.

Demande à être tenue informée dans un délai d'un an des modalités de mise en oeuvre du SNIIRAM.

Rappelle qu'elle devra être saisie de toute modification apportée au traitement.

[1] La liste des thèmes est disponible auprès de la CNIL.

V. DIFFUSION DE DONNEES PERSONNELLES SUR INTERNET

De nombreux sites Internet offrent un accès ouvert en ligne à des ressources documentaires contenant des informations de nature très diverses. Certaines des informations ainsi mises à la disposition de tous revêtent un caractère nominatif et peuvent quelquefois toucher à l'intimité de la vie privée de la personne. La CNIL, soucieuse des risques spécifiques que la diffusion de données sur support numérique est susceptible de poser a eu l'occasion, en 2001, de préciser des éléments d'une doctrine déjà esquissée depuis plusieurs années.

La Commission a en effet posé certaines limites à la diffusion de données « publiques » sous forme numérique lorsque ces données revêtent un caractère nominatif. Ainsi, si la Commission a admis, par exemple, que la plupart des mesures nominatives parues au *Journal officiel* puissent être accessibles par minitel, elle a cependant réservé un sort particulier aux décrets de naturalisation *[cf.* 15e rapport annuel 1994, p. 31). De même, lors du basculement du *Journa/ officiel* sur Internet, la CNIL a souhaité qu'outre les décrets de naturalisation, les décrets de changement de nom ne deviennent pas accessibles sur Internet.

Sur ce point, la réflexion de la Commission est bien entendu fonction de la nature des informations susceptibles d'être ainsi diffusées à tout public, mais elle est principalement commandée par les performances des moteurs de recherche qui permettent, lorsqu'ils sont interrogés sur le nom d'une personne physique, de retrouver dans l'instant, par un simple clic de souris, tous les documents, quel que soit leur format de diffusion sur le Web (html, pdf, image, etc.) mentionnant ce nom. Ainsi, de légitimes outils documentaires, les informations mises en ligne sur Internet peuvent se transformer en véritables « fichiers de renseignements » sur les personnes, pouvant être aisément utilisés lorsqu'il s'agit de se renseigner sur un candidat à l'emploi, à un logement ou à un crédit, sur un voisin ou un proche, et ce, à l'insu des personnes concernées. De surcroît, il est en pratique impossible de contrôler ou de limiter l'usage des informations une fois mises en ligne sur Internet.

La Commission doit évidemment rechercher le juste équilibre entre liberté d'accès à l'information et respect de la vie privée des personnes. Mais, dans certains cas — certes limités — ce souci d'équilibre la conduit à estimer, compte tenu des spécificités de la mise en ligne d'une information sur Internet, que la seule solution protectrice consiste à proscrire que les données soient diffusées sous leur forme nominative. Dans de telles hypothèses, l'information de fond peut bien évidemment être diffusée, mais la CNIL recommande que l'identité de la personne concernée soif occultée.

A. La diffusion sur Internet des décisions de justice

Les audiences des cours et tribunaux sont presque toujours publiques et les jugements et arrêts sont communicables à toute personne qui en fait la demande.

Pourtant, la compilation des décisions de justice sous la forme de bases de données et leur diffusion sur Internet soulèvent des interrogations particulières au regard de la protection des données personnelles.

Dès 1985, la CNIL avait été saisie des questions soulevées par l'utilisation des banques de données compilant les décisions de justice *[cf.* 6e rapport annuel 1985, p. 200). Le centre de documentation du barreau de Paris, qui offrait un accès aux bases de données diffusées par minitel, avait en effet relevé qu'un grand nombre d'interrogations des banques de données avaient pour objet de rechercher non pas toute la jurisprudence sur tel problème de droit, mais bien plutôt toutes les décisions se rapportant à une personne physique ou morale identifiée. D'outil de documentation, les banques de données juridiques devenaient ainsi de véritables fichiers de renseignements sur les personnes.

Afin d'étudier ces questions, la Commission avait organisé, en juin 1985, une table ronde réunissant les professionnels concernés, qui a été l'occasion de rappeler le droit reconnu à tout justiciable de revendiquer, au titre de la loi du 6 janvier 1978, l'anonymat des décisions de justice le concernant lorsqu'elles étaient diffusées ou accessibles sur support numérique.

La problématique de l'utilisation des banques de données juridiques s'est trouvée renouvelée avec le basculement de ces bases sur Internet. Les juridictions (Conseil d'État, Cour de Cassation, Cour des comptes, cours d'appel ou tribunaux) ou des éditeurs publics ou privés mettent en ligne sur Internet, de plus en plus fréquemment, des décisions de justice (jugements ou arrêts).

La CNIL, consciente que la poursuite de la réflexion qu'elle avait entamée en 1985 était devenue, à la veille de la mise en ligne gratuite de toutes les décisions de justice significatives dans le cadre d'un « service public de l'accès au droit », un réel enjeu de protection des données, a créé un groupe de travail chargé de procéder à toute audition utile avant de proposer des orientations à la Commission. Ainsi, des représentants du Conseil d'État, de la Cour de Cassation, de la Cour des comptes, de la chancellerie et du secrétariat général du Gouvernement, mais aussi de plusieurs éditeurs de banques de données de jurisprudence — les éditions Dalloz, la Gazette du Palais, Jurisdata, les éditions Francis Lefebvre, les éditions Lamy et la société Transactive — ont été auditionnés.

Au vu des conclusions présentées par le groupe de travail, la Commission a adopté, le 29 novembre 2001, une recommandation préconisant l'anonymisation des décisions de justice librement accessibles sur Internet.

Dans sa recommandation, la CNIL souligne les risques qu'une libre diffusion sur Internet de décisions de justice mentionnant l'identité des parties au procès ferait naître pour les droits et libertés des personnes concernées : par la seule mécanique des moteurs de recherche, c'est à un casier judiciaire universel, permanent et ouvert à tous que l'on aurait à faire face.

La loi « informatique et libertés » ne s'applique pas aux personnes morales. Pour les personnes physiques parties à un procès, la CNIL estime que la mise en ligne de l'information peut conduire à une « peine d'affichage numérique ».

Ainsi, la CNIL recommande que le nom et l'adresse des parties et des témoins soient occultés, dans tous les jugements et arrêts librement accessibles sur Internet, quels que soient l'ordre ou le degré de la juridiction et la nature du contentieux, dès lors que le site est en accès libre.

En revanche, la CNIL a tenu compte du fait que, s'agissant des sites en accès restreint (abonnement, *pay per view,* etc.) ou des CD-ROM de jurisprudence, par hypothèse, les décisions de justice ainsi mises à disposition d'un certain public ne sont pas référençables par les moteurs de recherche, nul ne pouvant y accéder « par hasard », c'est-à-dire sans même l'avoir recherché.

Aussi la CNIL s'est-elle bornée à recommander, dans de telles hypothèses, que l'adresse des parties, dépourvue d'utilité documentaire, ne figure plus sur de tels supports à l'avenir.

Cette recommandation a suscité de nombreuses réactions.

Certains soutenaient qu'elle interdirait désormais aux professeurs, aux étudiants, aux professionnels du droit d'évoquer un arrêt célèbre par référence au nom du demandeur. Il n'en est rien ; cette recommandation n'a nulle prétention à fixer des règles nouvelles de bons usages. La CNIL souligne que les audiences sont publiques, que toute personne peut se faire délivrer copie de l'intégralité d'une décision de justice, que sa recommandation ne s'applique pas aux recueils de jurisprudence sur support papier, pas davantage aux bases de données informatisées mises en oeuvre par les juridictions à un usage strictement interne. Sa portée est limitée aux problèmes spécifiques liés aux caractéristiques du réseau Internet et à celles des compilations de décisions de justice accessibles par le réseau international.

D'autres ont fait valoir que les recommandations de la CNIL limiteraient les possibilités de recherche sur Internet. La CNIL ne partage pas ce point de vue. En effet, les facilités de recherche désormais offertes par les bases de données (recherche en texte intégral, croisement de plusieurs mots clés, performances des indexations, etc.) ne devraient pas être perturbées par l'anonymisation des décisions de justice accessibles par Internet.

D'autres encore ont par ailleurs contesté la distinction entre sites gratuits et sites à accès payant, aboutissant, selon eux, à créer une distinction entre sites publics et sites privés, préjudiciable aux premiers.

Une telle analyse est très contestable. En effet, la distinction opérée par la CNIL ne vise nullement à créer un régime différent selon que le site est mis en oeuvre par un organisme public ou par un organisme privé. Le seul critère distinctif retenu par la Commission est la possibilité ou l'impossibilité de voir une décision de justice aisément indexée par un moteur de recherche.

Lorsque le site est en accès restreint ou lorsque la décision de justice figure sur un CD-ROM, l'information en cause ne sera accessible que si on la recherche spécifiquement. Elle le sera sans doute plus aisément qu'en la sollicitant auprès d'un greffe ou en consultant un recueil d'arrêts, mais dans des conditions de même nature. Bien sûr, comme certains contradicteurs l'ont souligné, il n'est pas exclu que la connaissance d'une telle décision sous sa forme nominative aboutisse à certains

mésusages. Mais cela est déjà vrai dans le monde non virtuel de l'accès aux décisions de justice.

En revanche, dès lors que le site est en accès libre, il y a un changement d'échelle et de nature : la décision de justice nominative indexable par tout moteur de recherche pourra être portée à la connaissance de tiers qui n'en avaient nullement sollicité la production. Elle sera forcément prise dans le « filet » de l'indexation automatique, alors même que le moteur de recherche avait été lancé au hasard, sous souci de rechercher l'éventuelle trace d'un jugement ancien.

Enfin, contrairement à ce que certains contradicteurs ont tenté de soutenir, la CNIL n'a en rien exonéré les éditeurs qui mettraient en ligne des bases de données de jurisprudence sur des sites Internet à accès restreint des obligations que la loi du 6 janvier 1978 leur impose. Ainsi, la CNIL a appelé leur attention sur les conséquences de l'application de la loi « informatique et libertés » lorsque leurs « produits » comportent le nom des parties : interdiction de mentionner les infractions et condamnations pénales, interdiction de faire apparaître, directement ou indirectement, les origines, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les moeurs des personnes (demandeur, défendeur, prévenu, accusé, témoin), reconnaissance du droit de s'opposer, pour des raisons légitimes, à voir figurer son nom dans une décision de justice diffusée sur support numérique, droit de rectification en cas d'information inexacte (ainsi, si la décision a été réformée en appel ou cassée).

Il résulte incontestablement d'un tel « corpus juridique » qu'une occultation du nom des parties sans être, dans cette hypothèse, explicitement préconisée par la CNIL, paraît seule de nature à éviter l'engagement d'actions en responsabilité contre les éditeurs.

En définitive, cette recommandation de la CNIL esquisse une orientation générale de nature à faire évoluer les esprits et, sans doute, certaines pratiques, dans le souci de la protection des données, conçue non pas comme un devoir théorique, mais avec les implications les plus concrètes dans la vie quotidienne : chacun devrait désormais être attentif à la mémoire ouverte que constitue Internet. Serait-il légitime que le nom d'une personne, initialement mise en cause pour un crime ou un délit, finalement reconnue en état de légitime défense et innocentée par ses juges, soit diffusé sur Internet et accessible à tous ? Peut-on être assuré qu'une décision de justice rendue accessible par Internet et comportant le nom des parties en litige dans un simple conflit de voisinage, tranché par le juge d'instance, ne serait pas susceptible de porter préjudice au défendeur ou même au demandeur ?

Il convient de souligner que le secrétariat général du Gouvernement a fait savoir à la Commission qu'il appliquerait, à l'occasion de la prochaine mise en ligne gratuite, dans le cadre du service public de l'accès au droit sur le site Internet Légifrance des décisions des cours et tribunaux, les recommandations de la CNIL en faisant procéder à l'anonymisation des décisions de justice qui étaient jusqu'alors diffusées de façon payante sur le site Jurifrance. Un délai de deux ans sera nécessaire. Cette résolution améliorera le sort des personnes physiques concernées.

Délibération n° 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence

La Commission nationale de l'informatique et des libertés ;

Vu la Convention 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 directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978;

Vu la délibération de la Commission n° 01-018 du 3 mai 2001 portant avis sur le projet de loi sur la société de l'information ;

Vu la communication présentée lors de la séance plénière du 30 novembre 1999 par M. Gérard Gouzes, vice-président ;

Entendus, lors des auditions effectuées par le groupe de travail présidé par M. Gérard Gouzes, vice-président, et composé de MM. Noël Chahid Nouraï, alors membre de la CNIL, conseiller d'Etat, Maurice Viennois, conseiller doyen honoraire à la Cour de Cassation, Pierre Leclercq, conseiller à la Cour de Cassation, et Didier Gasse, conseiller-maître à la Cour des comptes : M. Guy Canivet, premier président de la Cour de Cassation, M. Pierre Joxe, alors premier président de la Cour des comptes, M. Benoît Ribadeau-Dumqs, secrétaire général adjoint, représentant le vice-président du Conseil d'État, ainsi que des représentants des éditions Dalloz, de la Gazette du Palais, de Jurisdata, des éditions Francis Lefebvre, des éditions Lamy, de la société Transactive, ainsi que du ministère de la Justice et du secrétariat général du Gouvernement ;

Après avoir entendu M. Gérard Gouzes, vice-président, en son rapport et M^{me} Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La publicité des audiences, le caractère public des décisions de justice et la libre communication à toute personne qui en fait la demande des jugements et arrêts constituent des garanties fondamentales consacrées, notamment, par l'article 6 de la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales, et mises en œuvre, de longue date, par diverses dispositions du droit national.

Très tôt les plus hautes juridictions, mais aussi des éditeurs professionnels spécialisés, ont été amenés à réaliser une compilation des décisions les plus significatives rendues par les cours et tribunaux. Cette pratique est notamment suivie par la Cour de Cassation, depuis l'An II et par le Conseil d'Etat, depuis 1806, les éditions Dalloz annexant depuis 1837 aux recueils de jurisprudence qu'elles éditent, et dans le souci d'en faciliter la consultation, des tables alphabétiques au nom des parties à l'instance.

Le développement de l'informatique a considérablement facilité l'exploitation de la jurisprudence en permettant la création de bases de données juridiques. Ainsi, les juridictions ont, dès les années 80, constitué des bases de données enregistrant les décisions qu'elles avaient rendues, à des fins de recherche documentaire interne au profit de ses membres. Parallèlement, de véritables « banques de données » jurisprudentielles se sont développées, sur initiative publique ou privée, consultables par voie télématique sur abonnement.

C'est à cette époque que la CNIL avait été alertée sur le fait que les interrogations de ces bases de données, qui comportaient l'intégralité de la décision rendue, y compris l'identité des parties au procès, avaient quelquefois pour objet non pas la recherche de décisions présentant un intérêt juridique dans tel ou tel domaine, mais bien plutôt la recherche de l'ensemble des décisions de justice concernant une même personne. Ainsi, d'outils de documentation juridique, ces bases de données pouvaient être utilisées comme de véritables fichiers de renseignements.

À l'issue d'une réflexion d'ensemble menée en 1985, en liaison avec l'ensemble des juridictions et les éditeurs concernés, la CNIL a rappelé que les bases de données jurisprudentielles constituent, lorsqu'elles comportent l'identité des parties, des traitements automatisés d'informations nominatives au sens de l'article 5 de la loi du 6 janvier 1978 et doivent, à ce titre, être déclarées à la Commission.

La CNIL a par ailleurs rappelé les dispositions de l'article 26 de la loi du 6 janvier 1978 aux termes desquelles toute personne peut s'opposer, pour des raisons légitimes, à ce que des informations la concernant fassent l'objet d'un traitement automatisé.

Cependant, sensible au fait que les bases de données mises en oeuvre à l'époque étaient soit des bases internes aux juridictions sans possibilité de consultation extérieure, soit des bases accessibles par abonnement et/ou pour un coût relativement élevé — et, partant, principalement destinées aux professionnels du droit —, la CNIL n'a pas estimé devoir recommander que les décisions de justice enregistrées dans ces bases soient préalablement anonymisées. Une éventuelle préconisation en ce sens était apparue disproportionnée dans la mesure où le risque d'un usage des informations nominatives étranger à la finalité documentaire de ces bases était alors considéré comme faible, compte tenu des conditions de leur mise en œuvre.

Nouvelles technologies de diffusion de la jurisprudence : nouvelle réflexion

Des décisions de justice comportant le nom et l'adresse des parties sont aujourd'hui diffusées sur Internet.

Le faible coût des connexions au réseau (sans proportion avec le coût des liaisons minitel), la facilité de duplication de toute information diffusée sur Internet, l'impossibilité d'en contrôler l'usage à l'échelle du monde, et surtout l'utilisation de moteurs de recherche renouvellent incontestablement les termes de la réflexion engagée en 1985.

En 1985, on ne pouvait rechercher et obtenir une décision de justice qu'en se connectant à une banque de données juridiques et moyennant paiement d'une redevance. En 2001, il suffit d'interroger un moteur de recherche sur le nom d'une personne pour obtenir gratuitement l'ensemble des informations la concernant diffusées sur Internet à partir de sites géographiquement

épars ou de nature différente. Ainsi, dès lors qu'une personne est citée dans une décision de justice diffusée sur le réseau, et dans la mesure où cette décision aura été indexée par un moteur de recherche, elle deviendra directement accessible à tout utilisateur, alors même que tel n'était pas l'objet de la recherche et sans que l'internaute ait eu à se connecter à un site spécialisé.

Une réflexion que les performances des moteurs de recherche rendent plus aiguë encore

Les évolutions technologiques ont, depuis quelques années, modifié considérablement le mode de fonctionnement des moteurs de recherche sur Internet.

Initialement peu puissants, les moteurs de recherche de première génération n'étaient en mesure de retrouver les pages Internet que si ces pages avaient été préalablement référencées auprès d'eux par le responsable du site; à partir d'une liste de mots clés. Ainsi, s'agissant des sites diffusant de la jurisprudence, dès lors que les noms des personnes physiques n'avaient pas été préalablement référencés auprès des moteurs de recherche, aucune requête lancée à partir du nom d'une personne ne permettait d'avoir accès à une éventuelle décision de justice nominative la concernant.

Dans un deuxième temps, des moteurs de recherche, beaucoup plus puissants, ont permis de « balayer » les pages Web, en texte intégral, sans être alors limités par une indexation préalable de mots clés. Ainsi, ces moteurs de recherche peuvent indexer toute décision de justice comportant le nom d'une personne, même si l'auteur du site s'est attaché à ne pas référencer les décisions diffusées. Ces moteurs « de deuxième génération » connaissaient cependant une limite : seules les données diffusées au format html, langage de programmation universel sur Internet, étaient indexables, ces moteurs demeurant impuissants à rechercher des documents diffusés sous un autre format.

C'est cette dernière limite dont se sont affranchis les moteurs de recherche de la « troisième génération » actuellement disponibles sur le réseau. Très puissants et rapides, ils effectuent une recherche en texte intégral, sur tous les sites et, quel que soit le format de diffusion des données. Ainsi, le format pdf — format graphique de diffusion d'un texte sous la présentation d'une image — n'échappe plus à l'indexation. En outre, ces moteurs, qui effectuent une copie de l'intégralité des informations, lesquelles se trouvent ainsi conservées dans leur mémoire cache, permettent de consulter des informations diffusées sur un site alors même que ces informations ne seraient plus en ligne et n'auraient pas été dupliquées par un tiers. Ayant recherché et indexé une fois l'information, ces moteurs la conservent systématiquement.

Ces quelques éléments d'ordre technique donnent la mesure de ce qui est en cause : quels que soient la volonté ou le choix du responsable d'un site de jurisprudence sur Internet, accessible à tous, toutes les décisions de justice qui comportent l'identité des parties peuvent être indexées par les moteurs de recherche, qu'il y ait ou non référencement préalable de la décision, quel que soit le format de diffusion de celle-ci et même dans la circonstance où la mise en ligne aurait cessé.

C'est là que réside la véritable « révolution » provoquée par Internet, laquelle nécessite que des précautions particulières soient prises afin de préserver la vie privée des personnes : ce qui est techniquement possible lorsqu'une recherche documentaire via Internet est entreprise sur RABELAIS, l'est aussi lorsqu'il s'agit de se renseigner sur un candidat à l'emploi, à un lo-

gement ou à un crédit, sur un voisin ou un proche et ce, à l'insu des personnes concernées.

Le juste équilibre entre le caractère public d'une décision de justice et les droits et libertés des personnes concernées

La recherche de cet équilibre n'est pas nouvelle et les nombreuses dispositions de notre législation en témoignent.

Ainsi, des dispositions spéciales font interdiction de mentionner, à l'occasion de la diffusion ou la publication de certaines décisions de justice, dans des cas limitativement énumérés, le nom des parties. Il en est ainsi notamment pour certains procès en diffamation ou lorsque sont en cause des questions de filiation, des actions à fin de subsides, pour les procès en divorce, séparation de corps et nullité de mariage et les procès en matière d'avortement (loi du 29 juillet 1881 sur la liberté de la presse), pour les poursuites pénales exercées en matière de maladies vénériennes et de nourrice d'enfants (article L. 292 du code de la santé publique), pour les décisions prises à l'égard d'un mineur (ordonnance du 2 février 1945 relative à l'enfance délinquante), ainsi que dans le cas des victimes d'un viol ou d'un attentat à la pudeur, ou des personnes ayant fait l'objet d'une adoption plénière. L'énumération de ces contentieux particuliers souligne, à elle seule, la relative ancienneté de ces dispositions dérogatoires au droit commun qui, pour la plupart d'entre elles, sont intégrées à la loi sur la liberté de la presse et datent de plus de cent ans.

Sans avoir à prendre parti sur l'opportunité qu'une telle liste soit, le cas échéant, mise à jour par le législateur afin de mieux tenir compte de l'évolution des mentalités, des contentieux et des technologies de l'information, les spécificités du réseau Internet conduisent à repenser l'équilibre entre le caractère public des décisions de justice et les droits et libertés des personnes concernées, lorsqu'en tout cas ces décisions sont numérisées et accessibles par Internet.

En effet, il ne saurait être tenu pour acquis que, du seul fait de son caractère public, une décision de justice mentionnant le nom des parties, intégrée dans une base de données, puisse être numérisée et mise à la disposition de tous pendant un temps indéfini. Ainsi, le casier judiciaire national automatisé, qui constitue la mémoire des condamnations prononcées publiquement, est pourtant l'un des fichiers les plus protégés et les moins accessibles qui soit, dans le double souci du respect de la vie privée des personnes concernées et de la préservation de leurs chances de réinsertion.

En outre, si le juge a, pour certains contentieux déterminés, la possibilité d'ordonner l'affichage ou la diffusion par la presse écrite ou tout moyen de communication audiovisuelle de la décision rendue, celle-ci est strictement encadrée. D'une durée limitée dans le temps et devant être précisée par la décision elle-même, une telle mesure constitue, au moins en matière pénale, une peine complémentaire (article 131-10 du code pénal). La nécessaire protection de la vie privée des victimes explique également que la loi prévoit que leur identité ne peut figurer sur la décision affichée qu'avec leur accord ou celui de leur représentant légal (article 131-35 alinéa 3 du code pénal). Au regard de telles dispositions, la mise en ligne sur Internet de décisions de justice comportant le nom des parties ne constituerait-elle pas une nouvelle « peine d'affichage numérique » qui s'affranchirait de toutes les garanties prévues par les textes ?

Aussi, au-delà du caractère public de l'audience et de la décision elle-même, laquelle demeure communicable à toute personne qui en fait la demande, l'accessibilité universelle et permanente aux informations nominatives qu'elle comporte mérite-t-elle attention.

Les droits et libertés en cause

Les garanties reconnues aux personnes physiques par la loi du 6 janvier 1978 figurent au premier rang de ces droits et libertés.

Ainsi, l'article 31 de la loi subordonne la mise en mémoire informatisée de certaines informations qui « font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes », au recueil de l'accord exprès de l'intéressé, sauf autorisation par décret en Conseil d'État pris après avis de la CNIL pour un motif d'intérêt public. Or, des jugements et arrêts sont susceptibles de comporter des informations de cette nature lorsqu'elles sont intrinsèquement liées à l'instance en cause.

L'article 30 de la loi réserve aux seules autorités publiques ou aux personnes privées chargées d'une mission de service public la faculté de procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté.

Par ailleurs, la diffusion sur Internet, sous une forme nominative de jugements et arrêts, susceptibles d'appel ou de pourvoi en cassation, pourrait conduire les personnes concernées à intenter des actions en rectification, sur le fondement de l'article 36 de la loi, au motif que la décision du premier ressort aurait été réformée ou cassée et que l'accessibilité, à des fins qui peuvent largement excéder la seule recherche juridique, d'informations les concernant devenues inexactes, serait susceptible de leur porter préjudice.

De manière plus générale, l'article 26 de la loi reconnaît à toute personne physique le droit de s'opposer, pour des raisons légitimes, à ce que des informations la concernant fassent l'objet d'un traitement, ce droit ne pouvant être exclu, le cas échéant, que pour les seuls traitements publics ou mis en oeuvre par une personne morale de droit privé gérant un service public. Rapporté à la diffusion de décisions de justice revêtant un caractère nominatif, ce droit paraît pouvoir être revendiqué par des personnes qui souhaiteraient s'opposer à ce qu'une requête lancée sur leur nom par un moteur de recherche permette à quiconque de prendre connaissance, parfois plusieurs années après, d'un jugement les concernant dans un contentieux du licenciement, d'impayé, de responsabilité médicale, de trouble du voisinage, dans un contentieux fiscal ou pénal, pour ne citer que quelques exemples.

Au-delà des dispositions de la loi du 6 janvier 1978, d'autres droits et libertés pourraient être méconnus par une diffusion sur Internet des jugements et arrêts sous leur forme nominative. Ainsi, les effets qui s'attachent aux lois d'amnistie interdisent à toute personne ayant eu connaissance de condamnations pénales, de sanctions disciplinaires ou professionnelles ou d'interdiction, déchéances et incapacités effacées par l'amnistie, d'en rappeler l'existence sous quelque forme que ce soit ou d'en laisser subsister la mention dans un document quelconque (article 133-11 du code pénal).

Ces observations révèlent qu'un juste équilibre entre le caractère public d'une décision de justice et sa libre accessibilité sur Internet doit être recherché.

Une précaution minimale à l'heure des technologies de l'information : la suppression du nom des parties dans les jugements et arrêts rendus librement accessibles sur Internet

Le souci du juste équilibre ne saurait conduire à préconiser d'ôter tout caractère indirectement nominatif, au sens de l'article 4 de la loi du 6 janvier 1978, aux décisions de justice. Une telle orientation serait tout à fait disproportionnée, susceptible de nuire à la lecture de la décision ou contraindrait dans bien des cas à ne pas diffuser telle ou telle décision au motif que sa lecture seule permettrait d'identifier les parties en cause. Elle serait, par nature, contraire à la finalité légitime poursuivie par les juridictions ou les éditeurs de jurisprudence consistant à offrir un outil documentaire le plus complet et le plus accessible possible.

Ce même souci de l'équilibre ne serait pas atteint si le nom et l'adresse des personnes ayant été, d'initiative ou malgré elles, parties à un procès, continuaient à figurer sur les décisions de justice librement accessibles sur Internet, le plus souvent d'ailleurs sans qu'elles en aient conscience et sans qu'elles en pèsent les incidences.

Aussi, le nom et l'adresse des parties devraient-ils être occultés dans les jugements et arrêts diffusées sur des sites Web en accès libre, à l'initiative du diffuseur et sans que les personnes concernées aient à accomplir de démarche particulière.

Une telle préconisation ne paraît pas de nature à compromettre la recherche documentaire dans une proportion excessive au regard des intérêts en cause.

En effet, les facilités de recherche d'Internet permettent désormais très aisément à toute personne intéressée par la jurisprudence ou telle décision en particulier, de se connecter à un site spécialisé et de retrouver, par critères croisés, l'information pertinente. L'identification de la juridiction, la date de la décision, les articles de loi en cause, ou n'importe quel mot clé du texte intégral, constituent autant de critères de recherche efficaces. Aussi, plusieurs pays de l'Union européenne (Allemagne, Pays-Bas, Portugal) ont-ils déjà mis en œuvre une mesure d'anonymisation générale des décisions de justice publiées sur Internet. De même, la Commission de la vie privée belge a fait des propositions en ce sens au gouvernement belge. **Anonymiser quoi ?**

Le nom et l'adresse des parties et des témoins, dans tous les jugements et arrêts librement accessibles sur Internet, quels que soient l'ordre ou le degré de la juridiction et la nature du contentieux, mais cela seulement. Le principe de responsabilité morale et professionnelle conduit à considérer qu'il n'y a pas lieu, en tout cas au motif de la vie privée des professionnels concernés, d'occulter l'identité des magistrats ou membres des juridictions, ni celle des auxiliaires de justice ou experts, même si le risque de constitutions de « profils » de juges ou d'avocats à partir des décisions de justice publiées ne peut être exclu. Le risque qui s'attache à la numérisation ne paraît cependant pas supérieur à celui des circonstances qui forgent une réputation et sur lesquelles la CNIL ne dispose pas de moyens d'action particuliers. En revanche, les témoins devraient bénéficier de la mesure préconisée pour les parties.

Enfin, la protection des personnes morales ne relevant pas des attributions de la CNIL, il ne lui appartient pas de se prononcer sur ce point.

L'occultation du nom des témoins et personnes physiques parties à l'instance devrait être appliquée, quelle que soit la nature de la décision, le fait même d'avoir été partie ou témoin lors d'un contentieux civil, pénal, prud'homal, administratif ou autre, constituant une information propice au préjugé et qui révèle, en tout cas, la situation de conflit que, par nature, la décision de justice aura tranchée.

Le cas particulier des sites spécialisés en accès restreint et des CD-ROM de jurisprudence

Si l'accès du plus grand nombre à des décisions de justice nominative associé aux possibilités offertes par les moteurs de recherche sont de nature à faire redouter un usage des informations nominatives issues de ces décisions à des fins tout à fait étrangères à la recherche juridique, la restriction d'accès à certains sites spécialisés, qu'elle résulte de la mise en place d'une procédure d'abonnement préalable ou d'achat à la demande, et le coût d'un CD-ROM de jurisprudence paraissent de nature à éloigner un tel risque.

Aussi, un souci de mesure et de proportionnalité doit-il conduire à admettre qu'il n'y a pas lieu de préconiser que les décisions de justice déjà mises à disposition, dans ces conditions, se voient appliquer, rétroactivement, une mesure d'ensemble tendant à occulter l'identité des parties et témoins, quand ils y figurent, ce qui ne constitue pas le cas général.

Toutefois, et dans la mesure où l'adresse des parties figure parfois dans ces jugements et arrêts, alors même qu'elle n'est d'aucune utilité documentaire et qu'elle pourrait permettre de localiser la personne concernée, la Commission estime que l'adresse des parties devrait être occultée des décisions de justice qui seront à l'avenir diffusées sur CD-ROM ou sur un site Web spécialisé à accès restreint.

La seule occultation de l'adresse ne garantit évidemment pas les diffuseurs de décisions de justice sous forme nominative à l'égard d'éventuelles actions en responsabilité engagées par les personnes concernées à leur encontre. Ainsi, si les professionnels concernés devaient continuer à faire figurer le nom des parties dans les décisions de justice qu'ils éditent, il convient d'appeler spécialement leur attention non seulement sur la nécessité de déclarer leurs bases de données à la CNIL, mais aussi de rendre effectives les dispositions déjà citées des articles 30 (interdiction de procéder au traitement automatisé d'informations nominatives concernant les infractions, condamnations ou mesures de sûreté), 31 (interdiction de mettre ou conserver en mémoire informatique, sauf accord exprès des intéressés, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes), 26 (droit reconnu à toute personne de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement) et 36 (droit reconnu à toute personne de demander la rectification ou l'effacement d'informations la concernant) de la loi du 6 janvier 1978, sauf modification législative qui pourrait seule les en dispenser.

Cas particulier des organes de presse

La diffusion sur Internet d'articles de presse qui rendent compte du déroulement d'une instance judiciaire ou de certaines décisions de justice prononcées soulève, en terme de protection de la vie privée et de droit à l'oubli, des **difficultés de même ordre que celles qui ont été abordées s'agissant des ban-**

ques de données de jurisprudence, tout au moins lorsque les sites Web des organismes de presse sont accessibles à tout public. Un moteur de recherche ne distingue pas la nature du document numérique qu'il retrouve (décision de justice ou article de presse) et il suffit qu'un justiciable ait été cité une fois dans un journal pour que la numérisation et la mise sur Internet de ce journal le désignent à jamais et rappellent les circonstances dans lesquelles la personne concernée a eu à faire avec la justice.

L'article 33 de la loi du 6 janvier 1978 déroge expressément à certaines dispositions de la loi au bénéfice des organismes de la presse écrite ou audiovisuelle lorsque « leur application aurait pour effet de limiter l'exercice de la liberté d'expression ». Il en est ainsi pour les exigences posées en cas de transmission entre le territoire français et l'étranger, sous quelque forme que ce soit, d'informations nominatives faisant l'objet de traitements automatisés (article 24 de la loi), ainsi que pour le traitement des données sensibles (article 31 de la loi) et des informations relatives aux infractions et condamnations (article 30 de la loi). La directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données impose d'ailleurs aux États membres de prévoir, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme, des exceptions et dérogations « dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression. »

La Commission a notamment considéré, dans une délibération n° 95-012 du 24 janvier 1995 portant recommandation relative aux données personnelles traitées ou utilisées par les organismes de la presse écrite ou audiovisuelle à des fins journalistiques et rédactionnelles, que « les aménagements aux règles de la protection des données que commande le respect de la liberté d'expression ne doivent pas avoir pour effet de dispenser les organismes de la presse écrite ou audiovisuelle, lorsqu'ils recourent à des traitements automatisés, de l'observation de certaines règles. »

Sans que la présente délibération, circonscrite aux bases de données de jurisprudence, ait à arrêter les termes d'un éventuel compromis à rechercher entre liberté d'expression et droit au respect de la vie privée, il convient d'appeler l'attention des professionnels de presse concernés sur le changement de donne provoqué par Internet. La Commission forme le vœu que la réflexion déontologique puisse être entamée ou se poursuivre, à l'initiative des organes de presse et en concertation avec la CNIL, dans le souci de ménager la vie privée et la réputation des personnes concernées lorsque, en tout cas, la liberté d'information ne paraît pas nécessiter qu'elles soient citées nominativement.

Rappelle :
que les bases de données enregistrant sous forme numérique les déci sions prononcées par les juridictions constituent, si elles comportent le nom des parties, des traitements automatisés de données nominatives ; elles doi vent, à ce titre, être déclarées à la CNIL et respecter les dispositions de la loi du 6 janvier 1978 ;
qu'aucune disposition de la loi du 6 janvier 1978 ne prohibe la constitu tion, sous une forme nominative, de telles bases de données par les juridic tions ayant prononcé les décisions dès lors que l'accès à ces bases, quel qu'en soit le support (Intranet, postes dédiés, etc.), est exclusivement à usage

interne et réservé aux membres et fonctionnaires des juridictions concernées. **Estime qu'il serait souhaitable** :

— que les éditeurs de bases de données de décisions de justice librement accessibles sur des sites Internet s'abstiennent, dans le souci du respect de la vie privée des personnes physiques concernées et de l'indispensable « droit à l'oubli », d'y faire figurer le nom et l'adresse des parties au procès ou des témoins ;

— que les éditeurs de bases de données de décisions de justice accessibles par Internet, moyennant paiement par abonnement ou à l'acte ou par CD-ROM, s'abstiennent, à l'avenir, dans le souci du respect de la vie privée des personnes concernées, d'y faire figurer l'adresse des parties au procès ou des témoins.

En tout état de cause, appelle l'attention des éditeurs de bases de données de décisions de justice accessibles sur des sites Internet ou disponibles sur CD-ROM sur le fait que l'absence d'occultation du nom des parties ou témoins sur les décisions de justice doit conduire, d'une part, à déclarer ces traitements automatisés d'informations nominatives à la CNIL et, d'autre part, à respecter les dispositions de la loi du 6 janvier 1978 et tout particulièrement celles de ses articles 30 (interdiction de procéder au traitement automatisé d'informations nominatives concernant les infractions, condamnations ou mesures de sûreté), 31 (interdiction de mettre ou conserver en mémoire informatique, sauf accord exprès des intéressés, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes), 26 (droit reconnu à toute personne de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement) et 36 (droit reconnu à toute personne de demander la rectification ou l'effacement d'informations la concernant) de la loi du 6 janvier 1978.

Appelle l'attention des organismes de presse sur l'intérêt qui s'attacherait à ce que la mise en ligne, sur des sites Web en accès libre, de comptes rendus de procès ou de décisions de justice citant des personnes physiques parties ou témoins au procès suscite une réflexion d'ordre déontologique, en concertation avec la CNIL, lorsque, en tout cas, la liberté d'information ne paraît pas nécessiter la désignation nominative des personnes concernées.

B. La diffusion d'actes d'état civil datant de plus de cent ans sur Internet

En France, les actes d'état civil datant de plus de cent ans sont librement communicables à toute personne qui en fait la demande.

Les Mormons (l'Église de Jésus Christ des saints des derniers jours) ont entrepris, depuis plusieurs décennies, le microfilmage des registres d'état civil et paroissiaux dans la plupart des pays du monde. En France, ce microfilmage a été opéré dans des conditions fixées par un accord conclu entre la direction des Archives de France et la société généalogique de l'Utah (agissant pour le compte de l'Eglise de

Jésus Christ des saints des derniers jours) en 1960, modifié en 1987 après avis de la CNIL (cf. 8e rapport annuel 1987 p. 17).

L'accord conclu en 1987 prévoyait notamment que les microfilms ne seraient consultables par le public que dans le réseau des bibliothèques appartenant à la société généalogique et que toute copie de ces microfilms à des fins de délivrance à des tiers devait être soumise à l'autorisation écrite de la direction des Archives de France. Cette prescription était évidemment incompatible avec l'éventualité d'une diffusion sur Internet de ces données. Aussi la direction des Archives de France a-t-elle saisi la CNIL d'un projet d'avenant à la convention initiale afin, notamment, que certaines informations issues des microfilms puissent être mises en ligne sur le site Internet de l'Église de Jésus Christ des saints des derniers jours (http : //www.family-search.org).

Par délibération du 20 mars 2001, la Commission a pris acte que les informations appelées à être diffusées sur Internet étaient librement communicables en vertu de la loi française. Aussi, la Commission a-t-elle estimé que le transfert de ces données vers les États-Unis ne soulevait pas de difficulté particulière au regard des règles de protection des données.

La CNIL a toutefois précisé, dans un courrier adressé à la direction des Archives de France, que les mentions figurant en marge des actes d'état civil datant de plus de cent ans ne devaient pas être diffusées sur Internet.

La Commission a en effet relevé que les mentions portées en marge des actes d'état civil peuvent être de nature à révéler des informations sensibles sur la personne concernée tels les détails de sa filiation, ses mariages et divorces, ses changements de nom ou de nationalité, par exemple. La nature particulière de ces informations justifie d'ailleurs qu'elles ne soient pas portées sur les extraits d'actes d'état civil qui sont délivrés à toute personne qui en fait la demande.

Il aurait toutefois pu être soutenu que, dans la mesure où la loi fixant le délai à l'expiration duquel les actes d'état civil sont librement communicables ne distingue pas entre les informations figurant dans l'acte et celles figurant en marge, rien ne s'opposerait à la libre diffusion du tout sur Internet.

La Commission a cependant relevé que si l'article 7 de la loi du 3 janvier 1979 sur les archives dispose que les registres de l'état civil peuvent être « librement consultés » à expiration d'un délai de cent ans, la loi ne créait aucune obligation particulière pour les Archives de France de mettre à la disposition de tous de tels documents d'archives. À cet égard, la rédaction retenue dans le projet de loi sur la société de l'information paraît, encore, subordonner la communication d'archives publiques, dont le principe est rappelé et renforcé (« quels qu'en soient le support, le lieu de détention ou le mode de conservation »), à l'existence d'une demande préalable, laquelle détermine alors une communication « de plein droit » (cf. sur ce point l'avis de la CNIL sur le projet LSI, 21e rapport annuel 2000, p. 21). La libre consultation par chacun est une chose, la mise à disposition, une autre.

La Commission a, en définitive, considéré que la diffusion sur Internet des mentions marginales de l'état civil qui, bien que librement communicables, peuvent

revêtir un caractère sensible, était de nature à mettre en cause la vie privée des personnes concernées ou de leurs ayants droits, au moins en ligne directe et a demandé, pour ce motif, que les mentions marginales ne soient pas mises en ligne.

Délibération n° 01-015 du 20 mars 2001 portant avis sur un projet d'avenant à l'accord du 28 octobre 1960 modifié le 28 septembre 1987 conclu entre la direction des archives de France et la société généalogique de l'Utah

La Commission nationale de l'informatique et des libertés ;

Saisie par la direction des Archives de France d'un projet d'avenant modifiant l'accord conclu le 28 octobre 1960 et modifié le 28 septembre 1987 relatif au microfilmage par la société généalogique de l'Utah des registres paroissiaux et d'état civil de plus de cent ans conservés dans les services d'archives publiques françaises ;

Vu la Convention 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 directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu l'arrêté du 28 septembre 1987 approuvant l'avenant à l'accord du 28 octobre 1*960* entre la direction des Archives de France et la société généalogique de Salt Lake City ;

Vu les délibérations de la CNIL n° 82-106 du 6 juillet 1982, n° 85-88 du 17 décembre 1985, n° 86-85 du 8 juillet 1986, n° 87-44 du 28 avril 1987 ;

Vu le projet d'avenant présenté par la direction des Archives de France ;

Après avoir entendu Monsieur Alex Türk en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

Le microfilmage des registres paroissiaux (antérieurs à 1792) et d'état civil (datant de plus de cent ans) français par la société généalogique de l'Utah, initié en 1960 par un accord conclu entre la société généalogique de l'Utah et la direction des Archives de France, a été poursuivi dans des conditions fixées par la direction des Archives de France. L'accord initial a fait l'objet d'un avenant le 28 septembre 1987, pris après avis de la CNIL, fixant notamment les finalités d'un tel microfilmage, les conditions de délivrance de copies de ces microfilms et les personnes pouvant accéder à ces informations.

Le projet d'avenant dont est saisie la Commission a pour principal objet de permettre la diffusion, sur le site Internet de la société généalogique de l'Utah, d'informations issues des microfilms des registres paroissiaux (antérieurs à 1792) et d'état civil (datant de plus de cent ans) français. Les informations diffusées sont issues d'actes anciens, librement communicables à toute personne au sens de la loi du 3 janvier 1979 sur les archives, et concer-

nent les nom, prénoms, date et lieu de naissance, date et lieu de mariage, date et lieu de naissance de personnes pour la plupart décédées.

La Commission rappelle que le caractère public ou communicable d'une donnée personnelle ne prive pas les personnes concernées de la protection que leur offre la loi à l'égard de tous les traitements possibles de telles données.

En l'espèce, les données visées par l'avenant sont destinées à être transférées vers les Etats-Unis, pays ne pouvant être regardé comme assurant un niveau de protection adéquat au sens de l'article 25 de la directive du 24 octobre 1995.

La Commission observe toutefois que l'article 26-2 de la directive du 24 octobre 1995 dispose que de tels transferts peuvent avoir lieu lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties pouvant notamment résulter de clauses contractuelles appropriées.

Il y a donc lieu pour la Commission d'apprécier si les dispositions prévues dans l'accord conclu entre la direction des Archives de France et la société généalogique de l'Utah sont de nature à satisfaire aux conditions prévues par l'article 26-2 de la directive.

Prend acte :

que les informations diffusées se limitent aux nom, prénoms, date et lieu de naissance, date et lieu de mariage, date et lieu de décès des personnes ;

que ces informations concernent des personnes décédées et sont issues de documents d'archives librement communicables, en application des dis positions de la loi du 3 janvier 1979 sur les archives, à toute personne qui en fait la demande ;

que le microfilmage de tout autre document d'archives d'intérêt généalo gique devra être soumis à l'autorisation de la direction des Archives de France ;

que l'article 7 du projet d'avenant interdit toute exploitation commerciale directe ou par produit dérivé, par la société généalogique de l'Utah, des mi crofilms et que cette même interdiction pèse sur les tiers à qui la société pour rait délivrer des copies des microfilms ;

que la constitution de bases de données par la société généalogique de l'Utah à partir des informations issues des microfilms qu'elle détient devra être soumise à l'autorisation préalable de la direction des Archives de France ; qu'est interdit le croisement des bases de données qui seraient ainsi constituées avec toute autre base de données nominatives, sans qu'il soit né cessaire, au regard des dispositions de la loi du 6 janvier 1978, de sou mettre à l'avis de la CNIL la constitution de bases de données en l'état des obligations prescrites par la loi du 3 janvier 1979 sur les archives ;

que certaines catégories d'informations telles que l'origine ethnique des personnes ou leurs opinions religieuses ne peuvent être traitées ni diffusées au public ;

que toute difficulté née de l'application de l'accord sera résolue par la Justice française et selon le droit français.

Estime :

Au regard de l'ensemble de ces éléments, que ces dispositions sont de nature à assurer que le flux transfrontière de données en cause vers la société généalogique de l'Utah — États-Unis — sera réalisé dans des conditions assurant une protection de niveau équivalent à celle garantie par la loi française.

Demande :
— qu'à l'article 4 du projet d'avenant soit supprimé le groupe de mots « et de la Commission nationale de l'informatique et des libertés » ;
— que l'article 15 soit supprimé.

C. La diffusion sur Internet de sanctions administratives infligées par le ministère de la Jeunesse et des Sports

La CNIL a été alertée sur la diffusion, par le ministère de la Jeunesse et des Sports, sur son site, du bulletin officiel du ministère (le *BOJS)* qui comporte, notamment, la liste des personnes ayant été frappées d'une mesure d'interdiction d'exercer des fonctions d'encadrement dans les centres de vacances et de loisirs (« cadres interdits »). Ces mesures administratives, prononcées par le ministère, viennent sanctionner un comportement fautif, et peuvent venir en complément d'une condamnation au pénal de cadres qui auraient commis des infractions dans l'exercice de leurs fonctions.

La liste des personnes frappées par une telle mesure est normalement destinée aux directeurs de centres de vacances et de loisirs afin de leur permettre de s'assurer, lors du recrutement du personnel encadrant les mineurs qui leur sont confiés, que les candidats ne font pas l'objet d'une mesure administrative leur interdisant de telles fonctions. Elle était jusqu'à récemment accessible par minitel, au moyen d'un code d'accès que seuls détenaient les personnels habilités.

Or, par la mise en ligne sur Internet du bulletin officiel dans son intégralité, ces informations, dont le caractère sensible est évident, se sont trouvées librement accessibles à toute personne.

Or, s'il est impératif que les personnes frappées de telles mesures ne puissent plus exercer des fonctions d'encadrement de mineurs dans des centres de vacance, et que, dans cette perspective, la liste des personnes ainsi sanctionnées soit diffusée auprès des directeurs de centres, rien ne justifie, en revanche, qu'un employeur actuel ou potentiel, un voisin, ou un proche puisse, en interrogeant un moteur de recherche sur le nom d'une personne, apprendre, par « hasard », que cette personne est frappée d'une mesure d'interdiction.

Saisi par la Commission sur ce point, le ministère a décidé de suspendre la mise en ligne du bulletin officiel, dans l'attente de la mise en place d'un système permettant aux seules personnes habilitées (les directeurs de centres de vacances et de loisirs) d'y avoir accès.

Par ailleurs, et pour le même motif, seront également expurgés de la version du bulletin officiel mise en ligne sur le site Internet du ministère la liste des décisions du conseil de prévention et de lutte contre le dopage, les arrêtés d'interdiction ou d'injonction de cesser d'exercer la profession d'éducateur sportif et les sanctions disciplinaires prononcées par la commission disciplinaire, qui ont évidemment à être connus de certains professionnels ou organismes mais qui ne doivent pas être portés à la connaissance de tous.

D. La diffusion sur Internet d'une liste de « francs-maçons »

La CNIL a été saisie de la diffusion sur Internet de fichiers de membres d'obédiences maçonniques, internes à ces groupements, à l'insu des personnes concernées.

Plus de 3 000 noms et coordonnées ont été diffusés sur Internet, en infraction avec l'article 31 de la loi du 6 janvier 1978 qui interdit la mise en mémoire ou la conservation de données nominatives qui font, directement ou indirectement, apparaître, notamment, les opinions philosophiques des personnes.

Ainsi, une telle mise en ligne mettait l'auteur de la divulgation en infraction avec les dispositions de la loi et, tout particulièrement, avec l'article 226-19 du code pénal qui sanctionne le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître, notamment, les opinions philosophiques des personnes.

Seules les données manifestement rendues publiques par les personnes concernées font exception à cette règle.

Par ailleurs, les organismes de presse peuvent également traiter des informations sensibles lorsque ceci s'avère nécessaire à l'exercice de la liberté d'expression. En l'espèce, la CNIL n'a pas considéré que la mise en ligne du site litigieux relevait de cette exception et a entrepris, très vite, une action.

Saisie le 27 juin 2001 par le Grand Maître de la Grande Loge de France, la CNIL s'est fait communiquer, en vertu de ses pouvoirs propres, par l'hébergeur du site litigieux, les données de connexion qui lui ont permis d'identifier le créateur de ce site.

Il convient de relever que les listes nominatives ont été irrégulièrement diffusées au moins depuis le 23 juin 2001 et jusqu'au 27 juin, date à laquelle l'hébergeur, saisi par la Grande Loge de France, a pris toutes les mesures pour faire cesser cette diffusion.

Toutefois, la CNIL a estimé, compte tenu des possibilités de duplication ou de capture d'une information diffusée sur Internet qui sont sans limite, et malgré la fermeture du site litigieux, que la diffusion de telles informations sur Internet pendant plusieurs jours constituait « une atteinte manifeste à la vie privée et à la liberté d'association » qu'il convenait de porter à la connaissance du procureur de la République de Paris, en application des articles 40 du code de procédure pénale et 21 de la loi « informatique et libertés ».

La suite des événements a confirmé ces craintes, dans la mesure où plusieurs sites miroirs ont à leur tour, en Angleterre et en Belgique, permis d'accéder au fichier des francs-maçons en question. Grâce à la coopération des autorités de protection des données de l'Union européenne, le site miroir belge a été fermé rapidement.

Le parquet de Paris a fait savoir à la CNIL qu'une information judiciaire a été ouverte sur ces faits.

Il s'agit de la 18e dénonciation de faits au parquet à laquelle procède la CNIL et de la première dénonciation de faits commis via Internet.

Délibération n° 01-042 du 10 juillet 2001 portant dénonciation au parquet d'une infraction à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ; 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 directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu l'article 43-9 de la loi du 30 septembre 1986, modifiée par la loi du 1er août 2000 ;

Vu le règlement intérieur de la Commission et notamment ses articles 55 et 56;

Vu la délibération n° 01-039 du 28 juin 2001 de la Commission décidant une mission d'investigation destinée à identifier le responsable d'un traitement automatisé d'informations nominatives en infraction avec la loi du 6 janvier 7978 ;

Après avoir entendu Monsieur Michel Gentot, président, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Saisie le 27 juin 2001 par M. Michel Barat, Grand Maître de la Grande Loge de France, de la diffusion sur Internet des nom, prénoms, adresse, numéros de téléphone et indication de l'employeur de membres des loges composant cette obédience ;

Selon les informations portées à la connaissance de la Commission, plus de 3 000 noms et coordonnées de membres d'associations d'obédience maçonnique auraient été diffusés sur Internet depuis le site www.chez.com/listefm, au moins depuis le samedi 23 juin 2001. Cette diffusion de données à caractère personnel aurait continué jusqu'au mercredi 27 juin, date à laquelle l'hébergeur du site diffusant ces informations, saisi par la Grande Loge de France, a pris toutes mesures pour la faire cesser.

Devant veiller à ce que les traitements automatisés d'informations nominatives soient effectués conformément aux dispositions de la loi et tenant de l'article 21-2° de ladite loi, le pouvoir « de procéder, à l'égard de tout traitement, à des vérifications sur place et de se faire communiquer tous renseignements et documents utiles à sa mission », la Commission a décidé, par une délibération du 28 juin dernier, de procéder à une mission de vérification sur place auprès de tout prestataire technique afin de se faire communiquer toutes informations et documents de nature à permettre l'identification

de la personne qui aurait utilisé les services de l'hébergeur pour commettre cette infraction à la loi « informatique et libertés ».

Cette délibération a été notifiée au président de la société hébergeant le site par lettre du 30 juin 2001.

En réponse, ce dernier, tenu par l'article 21 de la loi du 6 janvier 1978 aux termes duquel « les dirigeants d'entreprises [...] ne peuvent s'opposer à l'action de la Commission ou de ses membres pour quelque motif que ce soit et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche », a communiqué à la Commission, le 2 juillet 2001, les informations devant être détenues et conservées en application de l'article 43-9 de la loi du 30 septembre 1986 modifiée par la loi n° 2000-719 du 1er août 2000, accompagnées de tous les éléments en sa possession relatifs à l'identité de la personne ayant procédé, par l'intermédiaire de son service d'hébergement gratuit, à la mise en ligne de données personnelles qui ne pouvaient l'être sans le consentement exprès des personnes concernées.

En l'état des éléments ainsi requis par la Commission, il n'y a plus lieu de procéder à l'exécution de la mission d'investigation qui se trouve ainsi satisfaite.

Au regard des éléments fournis, il est établi qu'un site a diffusé des informations relatives à plusieurs obédiences maçonniques parmi lesquelles figuraient de nombreuses informations à caractère personnel à savoir le nom, la profession, l'adresse, le numéro de téléphone fixe, le numéro de téléphone portable et l'identification de la loge d'appartenance. Par ailleurs, la copie des données de connexion a permis d'identifier la personne physique responsable de la mise en ligne de ces informations à caractère personnel.

La diffusion sur Internet d'informations révélant, sans que le consentement exprès des personnes ait été recueilli, leur appartenance, réelle ou supposée, à des associations à caractère politique, philosophique, religieux ou syndical constitue une atteinte manifeste à la vie privée et à la liberté d'association.

En l'espèce, la mise en ligne par le site litigieux de données personnelles révélant l'appartenance des personnes concernées à des associations de caractère philosophique met l'auteur de la divulgation en infraction avec les dispositions de la loi et, tout particulièrement, avec l'article 226-19 du Code pénal qui sanctionne le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître, notamment, les opinions philosophiques des personnes.

Les faits portés à la connaissance de la CNIL paraissent, à ce stade, suffisamment établis et constituent une atteinte caractérisée aux dispositions dont elle a pour mission d'assurer l'application.

En conséquence :

Décide, en application des dispositions de l'article 21 -4° de la loi n° 78-17 du 6 janvier 1978 :

— de dénoncer au parquet la mise en mémoire informatisée sur le site (www.chez.com/listefm) sans l'accord exprès des intéressés, de données nominatives qui, directement ou indirectement, font apparaître, notamment, les opinions philosophiques des personnes, fait susceptible de constituer l'infraction visée par l'article 226-19 du code pénal ;

— de transmettre au parquet l'ensemble des éléments d'identification de l'auteur supposé de l'infraction tels qu'ils résultent de l'accomplissement par la CNIL de ses missions.

VI. L'INTERNET ET LES MINEURS

Les bouleversements apportés par les technologies de l'information et de la communication dans la vie quotidienne de chacun, que ce soit à l'école, sur le lieu de travail ou au domicile, ont conduit la CNIL à s'interroger sur les mesures à prendre pour protéger les mineurs surfont sur Internet des risques d'atteinte à leur vie privée.

L'utilisation d'Internet par les enfants constitue indéniablement une source de préoccupation importante pour les parents et les éducateurs, conscients des dangers auxquels leurs enfants peuvent être confrontés sur le réseau du fait des contenus qui peuvent être illégaux ou de nature à les troubler (pornographie, racisme, violence physique et psychologique), de l'existence de messageries (avec la possibilité de contacts directs avec des tiers virtuels) ou du caractère marchand et commercial des sites. L'inquiétude des parents et éducateurs se trouve d'ailleurs souvent renforcée par leur manque de maîtrise des techniques et leur sentiment de ne pas être en mesure d'exercer leur autorité sur les enfants qui eux, surfent avec une grande aisance sur la toile. La Commission a pour sa part souhaité pointer du doigt un autre aspect : l'utilisation des enfants pour obtenir de manière déloyale des informations sur eux et leurs proches. En effet, la rapidité des échanges, l'interactivité, voire l'aspect ludique du réseau Internet font des enfants des cibles idéales pour se procurer des données toujours plus nombreuses et plus précises et ainsi constituer, à l'insu de leurs parents et sans que les enfants en aient eux-mêmes conscience, des bases de données très performantes sur l'environnement social et économique des familles, qui sont susceptibles de porter atteinte à leur vie privée.

Partant de ce constat, la Commission a souhaité prendre position sur la collecte de données personnelles auprès des mineurs via Internet. C'est l'objet du rapport adopté le 12 juin 2001 et disponible sur le site Web de la CNIL.

A. Le problème de la collecte des données personnelles

À l'occasion de ce rapport, la Commission a pu constater que toutes les actions entreprises ainsi que les réflexions en cours, notamment, au sein de l'Union européenne, sont axées sur les messages à contenu illicite et préjudiciable. Le plan d'action communautaire adopté par la décision du Parlement européen et du Conseil du 25 janvier 1999 a pour objectif de « promouvoir une utilisation plus sûre d'Internet et d'encourager, au niveau européen, un environnement favorable au développement de l'industrie liée à Internet ». Les actions projetées visent à développer les systèmes de filtrage, à inciter les industriels et les utilisateurs à mettre en place des codes de conduite et à encourager des opérations de sensibilisation à l'attention des

parents et des éducateurs. Mais, à aucun moment, le problème de la collecte de données personnelles auprès de mineurs n'est clairement posé.

Un seul pays se distingue en l'espèce : les États-Unis. Bien que n'étant pas doté d'une loi générale de protection des données, c'est le seul pays à avoir adopté une loi destinée à protéger les mineurs à l'égard de la collecte ou du traitement de leurs données personnelles : le *Children's Online Privacy Protection Act* (loi COPPA) officiellement entré en vigueur le 21 avril 2000.

Cette loi fédérale sur la protection de la vie privée des enfants de moins de treize ans est très contraignante. Elle interdit à tout détenteur de site de collecter des données personnelles auprès d'enfants de moins de treize ans sans autorisation parentale vérifiable. L'accord des parents doit être obtenu préalablement à la collecte, l'utilisation et/ou la cession des données. Le responsable du site doit par ailleurs afficher clairement sa politique en matière de protection des données (nature des données recueillies, utilisation des données et cessions envisagées). La page d'accueil du site ainsi que toutes les pages à destination d'enfants doivent comporter un lien vers le document décrivant la politique de protection des données et préciser le nom d'un contact dans l'entreprise. L'application de cette loi est contrôlée par la *Federal Trade Commission.* La méconnaissance de ses dispositions est susceptible de très lourdes amendes.

S'agissant de la France, la CNIL a tout d'abord fait le point sur les différents textes législatifs et réglementaires concernant les mineurs. Elle a ainsi pu constater que l'incapacité juridique du mineur ne signifiait pas dans tous les cas absence de droits. Le législateur a en effet permis aux mineurs ayant atteint un âge précis d'accomplir un certain nombre d'actes juridiques seuls ou avec l'autorisation de leur responsable légal (possession d'une carte bancaire dés 12 ans, consentement du mineur de 13 ans pour son adoption plénière ou une modification de son nom, signature d'un contrat de travail à 16 ans, droit au respect de son image...).

La Commission a ensuite, tout comme elle a fait connaître ses recommandations en matière de commerce électronique, de publipostage électronique, d'e-santé, et dans le monde du travail, souhaité dans le même esprit sensibiliser le public aux questions touchant à la protection des données personnelles des mineurs. Les propositions élaborées par la Commission dans son rapport ont donc pour objet de rappeler que les garanties offertes à tous par la loi du 6 janvier 1978 doivent s'imposer avec encore plus de force lorsqu'il s'agit de mineurs.

La Commission a examiné les différents types de collecte de données qui sont susceptibles d'être effectués auprès des enfants sur le Web afin de formuler, à l'attention des responsables de sites, des propositions très concrètes et d'une application aisée.

B. Les recommandations de la CNIL

S'agissant des « chat » ou des forums, qui visent les échanges réalisés en direct et de manière immédiate, la CNIL a estimé que la page d'accueil de l'espace de discussion doit rappeler aux utilisateurs éventuels des informations diffusées que ces

dernières ne peuvent être collectées ou utilisées à d'autres fins. Elle doit également informer les personnes de l'existence d'un droit d'accès et de rectification aux données les concernant (article 34 de la loi du 6 janvier 1978).

Lorsqu'un « chat » ou un forum est dédié aux enfants, le responsable du site doit non seulement s'abstenir d'utiliser pour son propre compte ou à des fins commerciales les méls échangés entre eux par les participants mais également avertir clairement les jeunes de ne pas donner leur adresse ni celle de leurs parents ou aucune autre donnée d'identification précise.

S'agissant de la collecte de données personnelles, il est rappelé que tout formulaire électronique de recueil de données nominatives doit mentionner le caractère obligatoire ou facultatif des réponses ainsi que le droit d'accès et de rectification. Lorsque les données collectées sont appelées à être cédées à un tiers à des fins de prospection commerciale, une mention doit figurer sur le formulaire afin que les personnes concernées en soient informées et mises en mesure de s'y opposer en ligne par une case à cocher. En l'absence de telles mentions, les données sont supposées n'être utilisées qu'en interne.

La CNIL a également considéré que serait excessif et déloyal tout mode de recueil par Internet de données personnelles visant à obtenir des enfants des informations sur leur entourage familial, le mode de vie des parents, leur statut.

De même, le recueil auprès des mineurs de données dites sensibles (origines raciales, opinions politiques, religieuses, philosophiques, syndicales, mœurs) doit être considéré comme interdit sauf si le responsable du site est en mesure de rapporter la preuve que les parents y ont consenti expressément.

La Commission considère également que la mise en ligne d'un jeu ou d'une loterie à destination des mineurs ne doit pas conduire le responsable du site à céder à des tiers les données recueillies à l'occasion du jeu sauf s'il est en mesure de rapporter la preuve que les parents ont expressément donné leur accord.

S'agissant de l'utilisation et de la diffusion d'une photographie d'enfant sur Internet, il est expressément rappelé que, quel que soit le support utilisé, elles ne peuvent être envisagées qu'avec l'accord de l'enfant et l'autorisation expresse de ses parents.

S'agissant des contacts que le site établit avec les enfants soit via leur adresse électronique, soit via une lettre d'information, il apparaît qu'aucune adresse électronique ne peut être utilisée à des fins de prospection commerciale ou autre si son titulaire n'a pas été informé, lors de la collecte, d'un tel usage et mis en mesure de s'y opposer aussitôt en ligne et gratuitement.

La CNIL recommande aux sites désireux d'entretenir des contacts avec un jeune, par le biais d'une lettre d'information, de ne collecter que l'adresse électronique et l'âge du mineur. Le recueil de toute autre information serait dans ce cas considéré comme non conforme à la finalité poursuivie.

C. La pédagogie à l'œuvre

La CNIL, comme il est d'usage, a, dans le cadre de la réflexion qu'elle a menée, consulté les principaux acteurs intervenant dans l'éducation et la relation avec les enfants. Si tous se sont montrés très désireux d'obtenir de la Commission des préconisations en la matière, ils ont tous insisté sur la nécessité de mener des actions de sensibilisation auprès des parents, des éducateurs et des enfants pour promouvoir une utilisation plus sûre d'Internet. La Commission, les rejoignant sur ce point, s'est prononcée en faveur de cette sensibilisation des mineurs, des parents et éducateurs aux questions de protection des données personnelles, en proposant notamment l'organisation d'une journée nationale d'information « Internet, jeunes et données personnelles » via les établissements scolaires et en liaison avec d'autres partenaires.

Cette sensibilisation a eu lieu à l'occasion de la fête de l'Internet, les 22, 23 et 24 mars 2002. Elle a pu être mise en oeuvre, sur l'initiative de la CNIL, avec le concours du ministère de l'Education nationale et la collaboration de la délégation interministérielle à la famille, l'Union nationale des associations familiales et 60 millions de consommateurs.

Elle s'est déroulée dans tous les établissements scolaires *[55* 000 écoles primaires, 15 *000* collèges et lycées) et s'est effectuée en trois temps :

— réflexion sur le thème de la protection de la vie privée et des données à caractère personnel ;
— réalisation par les enfants d'activités en ligne et hors ligne sur le même thème ;
— portes ouvertes aux parents le samedi matin.

Un matériel d'information a été mis à disposition des enseignants et du public.

Le site « juniors » de la CNIL a été actualisé pour cette opération et doté d'une nouvelle rubrique, une simulation dénommée « Trophée » destinée à sensibiliser les jeunes sur l'utilisation qui peut être faite des données qu'ils communiquent. De plus, un « kit » d'informations, téléchargeable à partir du site de la CNIL, a été également proposé.

Tous les partenaires ont installé, sur leur propre site Internet, un site miroir du site junior de la CNIL.

Le numéro de mars du journal *60 millions de consommateurs* a été consacré à « l'accès des jeunes à Internet » avec un dossier complet incluant la protection des données et les jeunes sur Internet.

Chapitre 3

LES DEBATS EN COURS

Au-delà de ses avis, délibérations, recommandations, la Commission mène une réflexion d'ensemble sur les nouvelles tendances technologiques et les problèmes qu'elles peuvent susciter. Instance de veille éthique et technologique, elle s'applique aussi à éclairer certains débats en cours. Les sujets traités à ce titre en 2001 n'étonneront pas : de l'identité numérique, qui se présente d'abord comme un nouveau marché commercial, aux technologies de la biométrie, qui sortent du champ policier auquel elles étaient jusqu'alors cantonnées, de l'administration électronique, « concept de l'année », aux « listes noires », qui ont toujours existé mais dont la prolifération dans tous les secteurs du commerce et des services appelle à une vigilance renouvelée, les réflexions qui suivent, quelquefois assorties des délibérations les plus importantes sur le sujet, ne ferment pas le débat. Elles s'efforcent de l'ouvrir ou de l'éclairer dans le souci d'une meilleure compréhension des enjeux.

I. LE MARCHE DE L'IDENTITE NUMERIQUE

Paul Valéry a pu dire du mot « liberté » qu'il était « de ceux qui ont fait tous les métiers ». Sans doute la sentence s'applique-t-elle aussi bien au mot « identité ».

Jadis, l'identité n'était qu'une « rumeur » faisant consensus. Vos proches ou votre voisinage pouvaient l'attester : on était qui on était parce que chacun en convenait. Le code civil conserve trace de cette histoire à travers la possession d'état, c'est-à-dire le témoignage humain confirmant ce que chacun observe et qui a valeur de preuve devant le juge, notamment en matière de filiation.

L'identité est désormais devenue affaire de techniciens à la recherche d'une preuve informatique de l'identité, d'un numéro d'identification, d'une carte d'identité

infalsifiable. Le temps n'est plus à la rumeur mais à la rationalité. On n'est plus qui on est parce que cela se dirait ; on est qui on est parce qu'un fichier informatique l'atteste.

Et le changement est radical : un lien social plus relâché, la crainte de la fraude, un appétit de rationalité, la multiplication des transactions à distance expliquent la tendance qu'illustre, par exemple, la délivrance de la carte nationale d'identité infalsifiable, véritable « parcours du combattant » tant les preuves à produire sont nombreuses — que l'on est qui on est, que l'on est bien Français, etc. — et tant paraît soudainement abolie la force probante de ce que l'on tenait jusqu'alors pour indiscutable : la présentation de son ancienne carte d'identité, le fait que l'on est inscrit sur les listes électorales, etc.

Les technologies en réseau, et singulièrement Internet, soumettent « l'identité numérique » à deux tensions contraires.

Une nécessité de s'identifier auprès d'un service distant pour éviter qu'un autre puisse se faire passer pour soi en accédant indûment à sa messagerie, à son compte fiscal, à son compte en banque, etc.

Mais aussi l'illusion de pouvoir jouer de son identité en s'avançant sous un pseudonyme dans les « chats » et les forums ou lorsque l'on se connecte à un site. « Internet crée de nouvelles frontières, plus difficilement perceptibles, à l'intérieur de chacun d'entre nous, à la faveur de ces « identités virtuelles » ces « masques » successifs que nous pouvons emprunter sur le réseau, dans un vaste carnaval de « la cyber-permanence » où nous jouerions entre le vrai et le faux, grisés parce que le philosophe Alain Finkielkraut nomme « la fatale liberté » a-t-il pu être dit[1] durant la XXXIII^{e} conférence internationale des commissaires à la protection des données qui s'est tenue à Paris en septembre 2001.

À cet égard, un sort mérite d'être fait à la réalité de l'anonymat sur Internet. En effet, si l'utilisation d'un pseudonyme ou la possibilité de se connecter à un site sans avoir à s'identifier peuvent être préconisées dans le souci de préserver l'anonymat à l'égard de tiers, cet anonymat n'est que relatif. La plupart des pays développés ont fait — ou font — obligation aux intermédiaires techniques — hébergeurs, fournisseurs d'accès — de conserver trace de nos connexions au réseau à des fins de sécurité; de police, de lutte contre la délinquance, le crime ou le terrorisme. Chacun peut tenter de se dissimuler — sans doute plus aisément sur Internet qu'ailleurs — mais précisément, les risques attachés à une telle dissimulation conduisent les États à mettre en œuvre un repérage technique de chacune de nos connexions. Le site de connexion, le forum ou le « chat » peuvent ne pas vous identifier, mais l'heure, la date de connexion et l'adresse « IP » qui aura été attribuée par le fournisseur d'accès à la connexion en cause seront conservées afin de permettre, le cas échéant, d'identifier l'ordinateur de l'utilisateur concerné.

Le discours sur l'identité numérique ne doit pas dissimuler les enjeux liés à la concentration de certaines de nos données personnelles entre de mêmes mains.

[1] Discours inaugural du président Michel GENTOT

Une tendance technologique à la normalisation et à la convergence y contribue : le souci de la mobilité (pouvoir accéder à Internet partout, depuis toute part, tout le temps) conduit à prendre en compte la variété des terminaux (PC, assistant numérique, Web TV, téléphone portable).

Parallèlement, le souci de la sécurité des transactions avec des procédés de signature électronique et les certificats numériques incite à la collecte de données personnelles.

Enfin, l'offre d'une plus grande ergonomie pour les utilisateurs que l'on souhaite dispenser d'avoir à saisir de manière répétitive des données personnelles (un « login », un mot de passe, un numéro de carte bancaire, une adresse physique) ouvre un marché technologique.

Ce sont ces tendances et les réflexions que suscitent les caractéristiques — toujours évolutives — de ce marché de l'identité numérique que le présent chapitre souhaite aborder.

A. Les tendances technologiques

1 — STANDARDISATION DES PROTOCOLES ET CONVERGENCES

Une standardisation de protocoles informatiques ou de télécommunication est en cours qui aura immanquablement des conséquences sur l'émergence de nouveaux identifiants, leur normalisation ou sur une nouvelle mise en relation de données personnelles.

Ainsi, des domaines sectoriels ou techniques jusqu'à présent séparés sont ou seront influencés par la standardisation en cours à l'échelle planétaire, comme le méta langage de description de données XML avec ses schémas de données normalisés ou les propositions de normalisation de l'IEEE *(Institute of Electrical and Electronics Ingineers),* le P1484.13 *Simple Human Identifiers* ou, de façon très exemplaire, ENUM.

Le protocole ENUM, porté par plusieurs organismes internationaux de normalisation des télécommunications et Internet, mérite d'être cité à ce titre. Les opérateurs de télécommunication sont spontanément sensibles à la culture de l'adresse universelle et à l'accès à valeur ajoutée. Le protocole ENUM décrit par l'IETF *[Internet Ingeneering Task Force,* instance de normalisation des protocoles Internet) consiste à utiliser un système unique d'adressage pour le réseau de télécommunication et le réseau Internet. Cette proposition de standard définit un cadre technique fondé sur le système des noms de domaines d'Internet accessibles à l'aide de la fonction DNS *(Domain Name Serveur)* permettant de faire correspondre à des numéros de téléphone (au format bien connu de chacun) des identifiants de services de communication ordonnés par priorité : adresse courriel, URL de site web, adresse SIP de serveur de téléphonie sur IP, messagerie vocale, autres numéros de téléphone...

Ainsi, la production d'un annuaire « virtuel » mondial commun aux domaines de la téléphonie et l'Internet n'est plus hors de portée de la technologie.

2 — VERS DES SERVICES D'AUTHENFICATION À L'ÉCHELLE DE LA PLANÈTE ?

Parallèlement à l'intégration de la mobilité et à la convergence progressive avec la téléphonie, les « services à accès » pourraient signer une tendance de fond du développement de l'Internet. Désormais, les services marchands d'une part, les applications à caractère communautaire d'autre part, pourraient être accessibles à un cercle plus restreint, sinon privé, d'internautes ou de mobinautes. Cette évolution est sans doute une réponse à l'actuelle crise que connaît le web.

En effet, le modèle économique du web reposant sur une communication libre et gratuite, rémunérée par l'audience et la publicité en ligne est en crise. À l'inverse, Internet en tant que système de transport des données ne cesse de croître et de s'affirmer avec des applications étrangères au web. Aussi, si le web représente aujourd'hui 45 % du trafic Internet, on admet communément qu'il n'en représentera plus que 10% en 2005.

Ces observations pourraient rendre compte, sinon de la difficulté d'opérer par le procédé de signature électronique une « greffe de confiance » dans un univers « anarchique » qui lui serait rétif[1] , du moins de la très grande complexité des architectures juridiques et professionnelles de la signature électronique, laquelle n'a, au demeurant, guère d'utilisateurs dans l'univers du web.

En revanche, l'encouragement de la signature électronique pourrait accélérer les évolutions en cours vers les « *Virtual Private Network »* (VPN), appelés quelquefois improprement « web services », qui correspondent non plus à un univers ouvert, homogène et universaliste, mais à un espace numérique fragmenté où les membres d'une communauté se retrouvent autour de fonctionnalités de « confiance interne ».

Cette fragmentation de l'espace virtuel rendra d'autant plus précieux, sinon indispensable, les « passerelles » entre nos multiples points d'entrée aux VPNs et un lien entre nos « identités numériques » partielles.

Dans ce contexte, les géants mondiaux de l'industrie informatique ont pris l'initiative d'offrir des solutions généralistes et à vocation universelle au travers de deux projets, jusqu'à présent concurrents, lancés au cours de l'année 2001 : Passport de Microsoft (comprenant des fonctionnalités autrement plus étendues que le service actuel éponyme) et Liberty Alliance autour d'un consortium animé par Sun Microsystèms sont actuellement en cours d'élaboration pour être intégrables aux nouvelles architectures de « web services ». Ces deux projets ont la même ambition professionnelle mais suivent, jusqu'à présent, deux approches différentes quant aux modalités de stockage physique (centralisé ou réparti) des données personnelles et quant à leurs modèles économiques respectifs. Les premiers résultats des travaux sont

---

1 L'univers « anarchique » du web à propos duquel la Cour fédérale de Pennsylvanie des États-Unis, dans une importante décision du 12 juin 1996, avait énoncé « tout comme la force d'Internet est le chaos, la force de notre liberté dépend du chaos et de la cacophonie, de la liberté d'expression sans entrave que protège le Premier Amendement [de la Constitution américaine établissant le principe de la liberté d'expression] »

attendus au cours de l'année 2002, mais les applications complètes d'envergure ne devraient pas être disponibles avant 2003.

Voilà un marché qui s'ouvre.

B. L'ouverture du marché

1 — LE « PASSPORT » DE MICROSOFT

Microsoft a révélé en 2001 sa nouvelle stratégie industrielle et commerciale médiatisée sous le nom de *Passport.* Il s'agit d'une architecture nouvelle que Microsoft a nommé *Hailstorm.*

Le schéma d'ensemble de « Passport » Microsoft

« Passport » était initialement conçu ou présenté pour permettre à chaque internaute d'enregistrer toutes les données personnelles qu'il est appelé à communiquer fréquemment lors de transactions en ligne (nom, adresse physique, mél, coordonnées bancaires), mais aussi le profil des terminaux informatiques dont il dispose (PC, assistant numérique de poche, portable), le cas échéant, ses sites préférés, le tout assorti de ses choix personnels en matière de protection des données personnelles tels qu'ils peuvent être définis par le protocole P3P mis au point par le consortium 3W. On se souvient que les logiciels mettant en oeuvre le protocole P3P permettent à un internaute de préenregistrer ses « préférences » en matière de politique de protection des données (par exemple : refus de conclure une transaction avec un site ne donnant aucune information sur l'usage ultérieur qui pourra être fait de ses données ou annonçant qu'il cédera ses données à des partenaires commerciaux, etc.).

Le préenregistrement dans « Passport » de telles informations aurait pour simple objet d'éviter à l'internaute d'avoir à ressaisir ses données personnelles lors de transactions sur Internet (achat de places de théâtre, réservation de billets d'avion, livraison à telle adresse, etc.) en ne s'identifiant qu'une fois selon la procédure habituelle du login et d'un mot de passe auprès de « Passport », les autres données d'identification réclamées par les sites associés, (sa banque, sa caisse de Sécurité sociale, les services municipaux, etc.) étant transmises automatiquement du serveur « Passport » au serveur du service. Bien sûr, seules les données pertinentes et non toutes les données rassemblées dans le « Passport » seraient alors transmises.

Microsoft se positionnerait ainsi comme interface « neutre » entre un internaute et un site web, qui gérerait les accès de l'internaute à tel ou tel site en fonction des choix personnels qu'il aurait mentionnés sur son passeport et de la politique du site en matière de protection des données personnelles.

En contrepartie, Microsoft s'engage à assurer la sécurité et la confidentialité des données figurant sur le « Passport » ainsi que, le cas échéant, la sécurité des transactions entre l'internaute et un site (chiffrement, signature électronique, etc.). Avec « Passport » et « l'orage de grêle », Microsoft souhaitait devenir un véritable « tiers

de confiance », de nombreux acteurs publics et privés ayant aussitôt été séduits par une telle offre de service.

Les premières réflexions sur cette offre commerciale

D'emblée, les commentateurs ou acteurs, parmi lesquelles les autorités de protection de données, ont soulevé certaines interrogations à propos d'une telle offre.

— *Un monopole laissant peu de place à la concurrence et aux Etats*

Compte tenu de la maîtrise de la technologie par Microsoft, de ses évolutions probables et de la gestion de l'accès des internautes aux sites web par une seule entreprise, le risque a été relevé que les États soient cantonnés à une situation de dépendance à l'égard de cette entreprise pour toute la régulation, voire le contrôle de l'Internet. Microsoft pourrait devenir, à titre d'exemple, le partenaire incontournable dans la lutte contre les atteintes aux droits de propriété intellectuelle, et pour l'ensemble des transactions chiffrées par « Passport », ces dernières pouvant être mises en œuvre sans passer par le pays de résidence d'un internaute (un internaute français faisant un achat sur un site web brésilien pourrait voir ses données personnelles transmises directement du serveur « Passport » établi aux États-Unis vers le serveur du site marchand établi au Brésil). Ainsi, les autorités judiciaires américaines et les agences de sécurité et d'information américaines seraient alors seules capables d'exercer un contrôle effectif sur les transactions et détiendraient un monopole en matière de régulation.

— *Des inquiétudes réelles sur le contrôle effectif du traitement des données personnelles*

La localisation du service « Passport » sur un serveur unique situé aux États-Unis n'est pas sans susciter des questions redoutables de droit national applicable et d'effectivité du contrôle des données ainsi conservées, tant par les autorités de contrôle européennes elles-mêmes que par les internautes.

Microsoft fait valoir cependant sur ce point que ces données ne seront jamais transmises à des tiers (partenaires commerciaux, etc.) et seulement utilisées lorsque l'internaute souhaitera les voir communiquer à un site avec lequel il est en contact. Par ailleurs, Microsoft prévoit que son offre européenne conduira à mettre en place des serveurs dédiés dans chaque État européen. Un tel schéma serait — il est vrai — plus rassurant. Il reste cependant que, par hypothèse, toutes les données enregistrées dans « Passport » seront regroupées sur un serveur unique, au plan national.

— *D'une offre commerciale à un « Passport » obligatoire ?*

Le système « Passport » ne devrait être utilisé que par les internautes qui le souhaiteraient. Cependant, certains aspects pratiques ou d'ergonomie, pourraient contrarier la réalité d'un tel choix. Tel serait le cas si l'option « par défaut » lors de l'installation de Windows XP était un « Passport » actif. Dans un tel cas, il reviendrait à l'internaute de désactiver « Passport », manipulation dont il n'est pas sûr qu'elle soit facile à opérer pour un utilisateur non averti. En outre, à supposer établi que

l'enregistrement dans « Passport » soit facultatif, il n'est pas exclu qu'un fournisseur de contenu lié à Microsoft subordonne l'accès à son service à la présentation de « Passport ». Dans une telle hypothèse, un internaute devrait activer « Passport » (c'est-à-dire livrer ses données personnelles) pour entrer en contact avec ce site web. Une fois ses données enregistrées dans « Passport », il est à craindre que l'internaute en reste là et ne le désactive pas, par choix, paresse ou négligence, surtout si des sites toujours plus nombreux exigeaient une telle procédure d'enregistrement. Dans cette hypothèse, le caractère facultatif de « Passport » serait un leurre.

Une fois « Passport » activé, et au fur et à mesure des achats de l'internaute, ce dernier contrôlera-t-il vraiment les informations qui seront enregistrées ?

— De *vives réactions*

Diverses plaintes ont été déposées contre Microsoft devant les juridictions américaines ou la FTC *(Federal Trade Commission).* Par ailleurs, l'Union européenne s'est saisie en août 2001 du problème posé par la position de monopole de Microsoft en tant qu'éditeur du système d'exploitation Windows. Une plainte de treize associations américaines, (notamment l'EPIC, *Electronic Privacy Information Center)* a été déposée auprès de la FTC sur des aspects spécifiques de protection des données personnelles faisant état, notamment, de ce que les demandes d'effacement des données enregistrées dans « Passport », déposées par des usagers, ne seraient pas traitées avant un délai d'un an.

— « *Passport » aujourd'hui.*

Cette application regroupe des données personnelles concernant 200 millions de personnes sont inscrites, dont 1,4 million en France essentiellement pour le service de messagerie Hotmail, propriété de Microsoft. Cependant, pour la grande majorité des inscrits, les données enregistrées sont peu nombreuses (numéro de carte bancaire, adresse postale, etc.).

Face aux réactions que la présentation de son projet a pu susciter, une nouvelle architecture est proposée par Microsoft ; le module d'authentification demeurait placé sous le contrôle de Microsoft, tandis que la gestion des données personnelles serait assurée par des fournisseurs de service indépendants.

2 — L'OFFRE CONCURRENTE DU CONSORTIUM LIBERTY ALLIANCE

Le projet « Passport » a suscité un projet concurrent initié par Sun Microsystème dans le cadre d'une association avec les acteurs des télécommunications (Nokia, Vodafone, France Telecom) et fabricants de cartes à puce (Gemplus, Schlumberger) et d'autres acteurs. La différence entre ce projet et « Passport » de Microsoft — au moins dans la version initialement présentée de ce dernier — consiste à proposer des briques logicielles en *open source* et non un service intégré propriétaire comme « Passport » et à ne pas prévoir de centralisation des données sur un serveur unique, les données personnelles étant distribuées chez les opérateurs.

L'Alliance, instruite par les réactions suscitées par le « Passport » de Microsoft, doit établir une charte à « caractère éthique » de nature contractuelle à l'égard de ses clients.

La CNIL qui est en contact avec les représentants français de ces deux projets en suit, en liaison avec ses homologues européens, très activement leurs évolutions et leurs développements.

Elle ne peut que se réjouir de la prudence réfléchie qui, après un temps marqué plutôt par le caractère attractif de la nouveauté des offres du marché, paraît désormais caractériser l'attitude commune des décideurs, au moins publics.

Les enjeux de la protection des données personnelles ne sont certes pas les seuls à être en cause. Mais dans ce domaine, nul ne contestera qu'ils soient d'importance.

II. LA « E-ADMINISTRATION »

L'administration électronique, la « e-administration » est aujourd'hui au coeur des politiques de réforme de l'Etat conduites dans la plupart des pays, en particulier en Europe, et constitue un axe prioritaire d'action de la modernisation administrative.

A. Considérations générales

Des programmes ambitieux se mettent ainsi en place dans la plupart des État européens, tous plus ou moins articulés autour des mêmes concepts, c'est-à-dire, la généralisation des formalités administratives en ligne, la possibilité pour chacun d'accéder à ces téléservices via un site portail unique éventuellement appelé à conserver pour chaque utilisateur un « compte citoyen », « coffre-fort électronique » gérant l'historique et le suivi de ses démarches administratives, enfin le développement de dispositifs d'identification et d'authentification reposant sur la signature électronique et sur des cartes d'identité électroniques.

À l'évidence, de tels projets, parce qu'ils impliquent nécessairement une multiplication des traitements de données personnelles, le développement d'interconnexions nouvelles voire la constitution de nouvelles bases de données centralisées, soulèvent en termes de respect de la vie privée, de préservation des libertés individuelles et publiques des enjeux fondamentaux et appellent à une réflexion approfondie. Le groupe de travail européen de l'article 29 de la directive européenne 95/46 a décidé d'entreprendre une étude commune sur l'ensemble de ces points, étude que la délégation française représentant la CNIL a reçu mission de coordonner.

1 — L'ADMINISTRATION ELECTRONIQUE A, EN FRANCE, PRÉCÉDÉ INTERNET

Le concept d'administration électronique est en effet sans doute un peu moins nouveau en France qu'ailleurs dans la mesure où notre pays dispose depuis plus de 15 ans à travers le minitel, d'une vraie culture de la transaction ou de la consultation en ligne. Pour ne donner que quelques exemples, on peut déjà, par minitel et ce depuis de nombreuses années, consulter le *Journal officiel,* s'inscrire dans une université, consulter des bases de données de jurisprudence mais aussi l'annuaire téléphonique ou encore réserver son billet de train...

À cet égard, l'application des règles de protection des données personnelles a indéniablement constitué un facteur de confiance dans le développement de cette « culture » de la transaction en ligne.

Mais Internet apporte incontestablement une autre dimension à ce concept et fait émerger de nouvelles problématiques.

Conscient de l'importance des enjeux en ce domaine, le Gouvernement a souhaité engager un large débat public afin notamment de faire émerger, si possible de manière consensuelle, les principales fonctionnalités et les garanties à apporter aux citoyens.

À cet effet, une mission, présidée par M. Pierre Truche, premier président honoraire de la Cour de Cassation, et composée de Monsieur Jean-Paul Faugère, préfet de la Vendée et de Monsieur Patrick Flichy, professeur de sociologie, a été mandatée par le Gouvernement pour préparer ce débat. À l'issue de nombreuses consultations et auditions en particulier de prestataires de services d'identification mais aussi de représentants d'administrations mettant déjà en œuvre des téléservices, cette mission a rendu public un Livre blanc, intitulé *Administration électronique et données personnelles.*

La CNIL a évidemment été associée à ces travaux, conformément à la lettre de mission du ministre de la Fonction publique et une synthèse de sa réflexion d'ensemble, portant notamment sur les interconnexions, le NIR et les téléprocédures figure en annexe du Livre blanc.

Depuis 1997, la CNIL s'est en effet prononcée sur de nombreux projets de télédéclarations par Internet, qu'il s'agisse des télédéclarations sociales par les entreprises (TDS NET), de la télétransmission des feuilles de soins (SESAM VITALE) — dont on dit aujourd'hui qu'elle représente la plus grande téléprocédure au monde — ou, dans le domaine fiscal, des télédéclarations de revenus, du télérèglement, de la télédéclaration de la TVA ou de l'accès en ligne au compte fiscal simplifié (programme Copernic, *cf. infra).*

La Commission a également été consultée par la chancellerie sur la mise en oeuvre d'un service permettant de solliciter par Internet la délivrance de certains extraits du casier judiciaire et de nombreuses collectivités locales l'ont saisie de la mise en ligne de certains services tels que l'inscription scolaire, la délivrance de fiches d'état civil, la prise de rendez-vous avec les services municipaux, etc.

2 — UN PREALABLE : NE PAS ABANDONNER LE LIEN SOCIAL AU VIRTUEL

Le développement de l'administration électronique ne doit pas porter atteinte au principe fondamental d'égalité des citoyens devant le service public. Il en résulte, comme l'ont souligné les ministres des États membres de l'Union européenne lors de leur déclaration du 29 novembre 2001 sur le Gouvernement électronique que :

— l'utilisation des téléservices doit rester facultative pour les usagers, au moins lors qu'il s'agit de personnes physiques ;

— elle doit se combiner avec les autres moyens d'intervention de l'administration (accueil physique, téléphone, écrit, bornes interactives...) ;

— la « dimension humaine » des relations usagers-administration doit, en tout état de cause, être préservée.

L'administration électronique devrait également être mise à profit pour « repenser », quand cela est nécessaire, l'organisation administrative ou « mettre à plat » la règle de droit, et devrait être, sinon le moyen, du moins l'occasion, de simplifier réellement les démarches administratives des usagers, et réduire la complexité administrative, et non de s'en faire complice comme la CNIL a pu le constater à diverses reprises.

Tel est le cas du contrôle des ressources pour l'octroi des prestations familiales. Ce contrôle systématique, prévu par la loi, conduit aujourd'hui les organismes sociaux à exiger de l'allocataire une déclaration de ressources qui sera rapprochée informatiquement de la déclaration de revenus faite à l'administration fiscale. D'un point de vue pratique, l'allocataire doit donc établir deux déclarations différentes. En outre, pour des raisons techniques ou de calendrier réglementaire, la comparaison entre les bases de données n'est pas opérée sur la même année de référence. Aussi, la CNIL a-t-elle encouragé, lors de l'examen de l'interconnexion entre ces deux fichiers, la fusion de ces deux déclarations en une seule.

Les interconnexions de fichiers dans lé domaine social ont pour objet principal de contrôler a posteriori la cohérence entre diverses obligations déclaratives. La CNIL n'a jamais contesté la légitimité de cet objectif mais elle a également estimé nécessaire de recommander que la mise en place des interconnexions soit l'occasion d'envisager, en manière de contrepartie, de réelles simplifications des démarches administratives[1] pour les usagers. Ainsi, la CNIL a pleinement approuvé les échanges d'informations instaurés, depuis 1995, entre la Caisse nationale d'assurance vieillesse et la Direction générale des impôts, afin que les avis de non-imposition puissent être obtenus directement sans que les retraités aient, comme auparavant, à les adresser eux-mêmes à leur caisse de retraite[2].

---

[1] Cf notamment en ce sens la délibération du 25 mars 1997 portant avis sur un projet d'article L 115-8 du code de la sécurité sociale posant le principe d'échanges d'informations entre l'administration fiscale et les organismes de protection sociale (texte non adopté en raison de la dissolution de l'Assemblée Natio nale).

[2] Ces informations sont exclusivement utilisées pour déterminer les taux de prélèvement à appliquer sur les pensions de retraites ou d'invalidité au titre des contributions et cotisations sociales.

Les exemples pourraient être multipliés.

L'usager, souvent désemparé devant une réglementation de plus en plus complexe, perdu dans le dédale des démarches administratives, s'en remet le plus souvent à l'administration et à l'informatique pour déterminer ses droits, établir, en ses lieu et place, déclarations, feuilles de paie, précompte des cotisations.... Le système de gestion des prestations familiales l'illustre : sous l'effet des législations sociales successives, 15 000 règles seraient actuellement en vigueur : elles ne pourraient, à l'évidence, être appliquées sans l'aide de l'outil informatique.

Aussi est-il à espérer que le développement de l'administration électronique puisse s'accompagner d'un effort véritable pour, tout à la fois, réduire le nombre de formalités et des pièces justificatives à produire et favoriser une meilleure compréhension des formalités par les usagers en leur fournissant, sur tous supports disponibles et en langage clair, les moyens de déterminer eux-mêmes l'étendue de leurs droits et obligations.

Mais au-delà, le concept, sinon le slogan, « d'administration électronique » peut conduire certains à s'interroger sur la pertinence des principes fondamentaux de protection des données personnelles à l'heure du « tout numérique ».

La CNIL est, bien évidemment, à la place qui est la sienne, ouverte à des interrogations de cette nature, mais sans doute faut-il éviter quelques idées fausses ou illusoires dans le souci de « dévirtualiser » ces débats.

3 — DE QUELQUES IDEES A LA MODE

« Devenons propriétaires de nos données » ou la maîtrise de ses données par la personne elle-même

Le problème de la propriété des données personnelles est posé de toute part, (qui est propriétaire des données, celui qui les communique et auquel elles se rapportent ou le responsable du fichier auquel elles ont été communiquées et qui les détient ?) comme si ce concept pouvait être opératoire. Sans doute est-il directement inspiré d'une certaine philosophie américaine du commerce des données et, en tout état de cause, d'une certaine privatisation de la protection des données, entendue comme le triomphe des droits subjectifs. La CNIL a déjà souligné certaines tendances du marché en ce domaine consistant à rétribuer les personnes, par des cadeaux, des services offerts, des réductions, en contrepartie de l'abandon par la personne concernée de ses droits sur les données qui la concernent ou la caractérisent. Puisque les données personnelles ont acquis une valeur marchande, il suffit de les acheter directement à la personne concernée ; tout propriétaire peut aliéner son bien ! C'est la vie privée en « libre service ».

De même l'idée d'une meilleure maîtrise des données par la personne elle-même est-elle abondamment soutenue. À ce titre, l'illustration la plus fréquemment rencontrée est la suivante : l'administration électronique permettrait, enfin (!), aux personnes d'exercer effectivement leur droit d'accès. Les tenants de cette thèse font en effet valoir que le droit d'accès est actuellement peu exercé, que ce soit par

ignorance de ce droit, en raison de la lourdeur des démarches à entreprendre, ou encore d'éventuelles ou supposées réticences des administrations à communiquer les informations.

L'idée que les données conservées par les administrations pourraient désormais, grâce à Internet, être accessibles directement par l'usager, présente incontestablement un intérêt. Mais ne peut-on soutenir que si le droit d'accès est peu exercé, en pratique, c'est qu'au fond l'essentiel pour nos concitoyens n'est pas tant de vérifier la teneur des données qu'ils ont le plus souvent communiquées eux-mêmes à l'administration concernée, que d'avoir la garantie que ces données ne seront pas détournées de la finalité initiale, communiquées à des tiers qui n'ont pas à en connaître ou leur seraient opposables de nombreuses années après. À cet égard, les garanties essentielles offertes par les législations de protection des données ne sauraient être considérées comme satisfaites au seul motif qu'un droit, certes important, pourrait être plus commodément exercé.

Y a-t-il lieu, en définitive, de soutenir que l'usager bénéficierait, dans la sphère administrative, d'un véritable droit à l'autodétermination de ses données ? Certains avancent que l'usager pourrait, très largement au-delà du droit d'accès, disposer d'un droit de regard sur l'utilisation de ses données administratives, voire même du droit d'en contrôler l'usage, de consentir à telle ou telle communication de données et de déterminer les administrations qui auraient « droit » à connaître ses données et celles qui devraient en être « privées ».

Ne s'agit-il pas d'un leurre pouvant donner à l'usager le sentiment erroné qu'il serait seul maître d'en décider alors que l'administration constitue à l'évidence un champ d'intervention où l'usager peut être contraint, par la loi et les règlements, à communiquer des données à l'administration, celle-ci étant en droit de les exiger, ce que reconnaît d'ailleurs le deuxième alinéa de l'article 26 de la loi de 1978. Cette disposition prévoit en effet, s'agissant des traitements du secteur public, que les personnes concernées peuvent se voir privées de l'exercice de leur droit d'opposition à ce que des données les concernant figurent dans un traitement.

La directive européenne 95/46, si elle consacre bien en son article 7, le consentement de la personne comme une des conditions légitimant un traitement de données, prévoit également que le traitement est légitime s'il est nécessaire au « respect d'une obligation légale à laquelle le responsable du traitement est soumis » ou encore à « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique », ce qui est le cas de nombreux traitements de l'administration et en particulier des interconnexions mises en place entre administrations pour, par exemple, contrôler les déclarations des administrés.

Aussi le discours autour du « consentement » ou de la « maîtrise de ses données par la personne » elle-même appelle-t-il de fortes réserves que le Livre blanc sur l'administration électronique a d'ailleurs opportunément énoncées. Promouvoir le consentement ne risque-t-il pas de donner à croire que chacun serait libre de ne pas figurer dans un fichier fiscal, un fichier de police, un fichier de gestion administrative ? Ce serait tromper nos concitoyens sur la réalité de leurs droits et peut-être sur l'essentiel de ce qui constitue le lien social qui contraint à devoir concilier vie privée

et d'autres valeurs d'intérêt général, même lorsque le bénéfice attendu n'est pas, comme dans la sphère marchande, individuel et immédiat (un bon de réduction) mais collectif et à moyen ou long terme (une redistribution moins inégalitaire des revenus, un surcroît de sûreté dans la cité ou un meilleur service rendu aux usagers des services publics).

En sens inverse, promouvoir le consentement, ne peut-il aboutir à anéantir des garanties d'intérêt public au motif que les personnes auraient consenti ? Ce serait là renvoyer le faible au fort, et tromper alors nos concitoyens sur l'effectivité des garanties destinées à les protéger.

« D'une administration en silos à une administration en réseaux »

La e-administration, c'est aussi la priorité donnée à l'interopérabilité des systèmes d'information, à un décloisonnement des fichiers, bref à un plus grand partage de l'information désormais accessible à un nombre d'utilisateurs de plus en plus important. Certains évoquent ainsi l'idée qu'avec Internet on pourrait passer d'une administration en « silos » à une administration en réseaux.

Soit, mais le problème est davantage celui du « silo » — c'est-à-dire le rassemblement dans une même base de données d'informations jusqu'à présent cantonnées en fonction d'une finalité définie avec précision — que celui de la mise en « réseaux ». La mise en œuvre du fichier STIC du ministère de l'Intérieur recensant la quasi-totalité de l'information de police judiciaire jusqu'alors collectée en France mais dans des fichiers épars illustre le caractère aigu des problèmes posés à ce titre. Focaliser sur un heureux passage à une administration en réseaux, c'est peut-être distraire l'attention de la difficulté à rassembler toute l'information disponible dans une même base commune, « en silo ». L'illusion de cette « idée à la mode » est celle qu'entretient l'opposition, en réalité très artificielle, entre « silos » et « réseaux ».

Comment peut-on garantir la confidentialité des informations si elles deviennent accessibles à un très grand nombre d'utilisateurs ? Comment peut-on éviter des détournements de finalité lorsque des informations collectées pour des fins différentes se voient rassemblées dans une base commune ? Ne peut-on craindre, alors, que ne se profile à nouveau le risque d'une interconnexion généralisée des fichiers administratifs, d'un SAFARI bis ?

Ce débat est essentiel. Le poser en termes clairs ne signifie nullement qu'il faudrait s'en tenir à une position de principe hostile à tout décloisonnement administratif ou à une position dogmatique préférant des bases de données étanches à des bases de données communicantes. Un plus grand partage de l'information peut aussi présenter des avantages pour le citoyen comme le projet « Copernic » du ministère de l'Économie et des Finances en témoigne *(cf. infra)*.

Certes, aucun principe de protection des données personnelles n'interdit les interconnexions. Mais le principe de finalité justifie les précautions particulières prises en matière d'interconnexions de fichiers ou de regroupement dans un même ensemble d'informations provenant de fichiers distincts. Ainsi, la plupart des législations de protection des données soumettent les interconnexions entre fichiers à

finalité différente fussent-ils détenus dans le cadre d'une même administration, à un régime particulier de contrôle par l'autorité de protection des données. Tel est le cas en France.

Dès lors que les droits des personnes concernées sont reconnus et que des mesures de sécurité appropriées sont prévues, la CNIL admet que certains fichiers puissent être interconnectés si un intérêt public prédominant le justifie, étant observé qu'une vigilance particulière s'impose si les informations susceptibles d'être rapprochées sont protégées par un secret professionnel. Dans ce cas l'échange d'informations couvertes par un secret (bancaire, social, fiscal) ne peut intervenir que si ce secret est préalablement levé. Il ne saurait être dérogé à un secret prévu par la loi du seul effet de la technique.

S'il peut donc être admis que des interconnexions puissent être mises en œuvre, dans les conditions précédemment définies, pour répondre à des finalités déterminées, une interconnexion généralisée de l'ensemble des fichiers publics n'est pas envisageable sauf à remettre en cause le fondement même de la protection des données personnelles.

4 — POUR UNE REFLEXION RENOUVELEE SUR LES IDENTIFIANTS ?

Certains considèrent que le débat sur l'administration électronique est l'occasion de s'interroger sur le point de savoir s'il ne convient pas d'adopter un dispositif d'identification unique pour accéder à l'ensemble des téléservices publics.

On voit d'ailleurs apparaître des offres techniques de gestion de l'identité numérique, reposant sur des procédures simples, voire uniques, d'identification et d'authentification.

On peut résumer la position de la CNIL sur cette question des identifiants par la formule : à chaque sphère son identifiant ; pas d'utilisation généralisée d'un numéro national d'identification. Et force est de constater qu'aujourd'hui l'accès aux téléservices publics existants s'effectue selon les dispositifs d'identification spécifiques aux systèmes d'information de chaque service public concerné (et acceptés par la CNIL), que l'usager a l'habitude d'utiliser dans le cadre de ses relations « traditionnelles » avec chacun de ces services.

Il ne semble pas que l'on s'oriente vers un bouleversement des pratiques en ce domaine.

Sur ce point les premières conclusions du Livre blanc sur l'administration électronique et les données personnelles manifestent un souci de précaution et de réalisme, souci que partage pleinement la Commission. Les propos tenus, au Printemps 2002, par le ministre de la Fonction publique sont à cet égard précis : « l'identité numérique n'est et ne peut pas être unique, pas plus que l'identité au sens traditionnel des relations « papier » avec l'administration. De la même façon que nous disposons aujourd'hui, entre autres, d'un numéro de Sécurité sociale, d'un numéro fiscal, d'une carte d'identité, d'un passeport, autant d'identifiants distincts

les uns des autres, nous aurons demain plusieurs identifiants électroniques. Ce serait une vision naïve de la numérisation que de croire qu'elle mène naturellement à l'unicité de l'identité [...] ». Pour illustrer son propos, le ministre a utilisé la formule de « porte-clefs électronique ». S'il y a plusieurs clés (d'interrogation de bases de données) c'est qu'il n'y a plus un seul « coffre-fort » de nos données personnelles !

5 — JUSQU'OU PEUT ALLER LA PERSONNALISATION DES TÉLÉSERVICES PUBLICS ?

Derrière le concept de « coffre-fort électronique » (ou compte citoyen) apparaît l'idée que l'individu pourrait faire conserver (« notariser ») par un tiers ses données personnelles (son dossier administratif, son dossier médical...).

Une telle démarche est-elle viable et opportune ? Est-on prêt à confier à un tiers le soin de conserver ses données, l'historique de sa situation administrative, sociale, professionnelle, de ses antécédents médicaux... ? Ces interrogations ne sont pas minces.

Se pose de façon corollaire la question de la nature exacte des données qui pourraient être ainsi regroupées et des conditions de leur utilisation. Au regard des règles de protection des données, un juste équilibre doit être trouvé pour, tout à la fois, faciliter et personnaliser les démarches administratives et éviter le recueil et la conservation en un point unique d'informations personnelles sur les administrés. Ainsi, l'adresse physique est loin d'être neutre. Si chacun dispose d'un « compte électronique », n'en vient-on pas à créer de fait ou de droit un véritable fichier de domiciliation, question qui a toujours, en tout cas en France, été sensible. De même, dès lors que le dispositif mis en place permettrait de « tracer » les différentes démarches administratives effectuées par l'usager, on peut s'interroger sur l'usage qui pourrait être ainsi fait de ces « traces ». Enfin, à qui pourrait être confié le soin de gérer ces « coffres-forts électroniques » ? L'État ? Des prestataires privés ?

Il doit être noté que sur l'ensemble de ces questions, la position du Gouvernement semble très prudente, la formule du coffre fort électronique, un temps retenue, ayant été très largement nuancée au profit de celle de « point d'entrée personnalisé et unique ».

6 — QUELLES EXIGENCES DE SECURITE POUR L'ADMINISTRATION ÉLECTRONIQUE ?

La sécurité juridique des transactions passe incontestablement par l'authentification et l'identification des personnes. Mais, à cet égard, une première règle s'impose : le respect, dans la mesure du possible, de l'anonymat : toutes les démarches administratives ne nécessitent pas d'identification.

On doit en effet s'interroger sur l'utilité et l'opportunité qu'il y aurait à prévoir une certification obligatoire et systématique de tous les échanges avec l'administration et donc à rendre nominatives l'ensemble des relations des usagers avec

l'administration, ce qui pourrait conduire à une modification radicale de la situation actuelle, alors même que, de surcroît, de nombreuses démarches administratives sont effectuées par des tiers (cas par exemple des procédures d'immatriculation des véhicules, réalisées en pratique par les concessionnaires mandatés à cet effet par leurs clients ou de nombreuses démarches sociales effectuées par les assistantes sociales).

En tout état de cause, il doit être possible de demander en ligne des formulaires qui sont par ailleurs disponibles librement auprès de l'administration ou de consulter un document administratif communicable sans avoir à s'authentifier auprès de l'administration.

Les exigences de sécurité techniques doivent à l'évidence être modulées en fonction du type de démarche administrative entreprise qui, pour certaines, ne nécessitent sans doute pas une authentification forte.

Certes, la reconnaissance récente, dans notre droit interne, des procédés de signature électronique reposant sur des infrastructures à clé publique, s'est traduite, dans les avis rendus par la CNIL depuis 2000 sur la mise en oeuvre des télédéclarations fiscales, par des recommandations fortes sur l'utilisation de tels procédés[1]. La CNIL s'était déjà prononcée favorablement en 1998, sur l'utilisation de la carte du professionnel de santé, pour signer, de façon électronique, les feuilles de soins télétransmises aux caisses de Sécurité sociale.

Mais le recours systématique à des procédés de signature électronique ne constitue pas aujourd'hui, pour la CNIL, une condition préalable à la mise en place des téléprocédures. Elle est indispensable là où un impératif d'authentification s'impose dans le souci de la confidentialité des données et pour éviter toute usurpation d'identité. Elle n'a pas à être systématiquement imposée dans l'ensemble des démarches administratives.

Tant que le droit, la technique et l'économie des infrastructures à clé publique ne seront pas totalement stabilisés, il pourrait paraître prématuré d'imposer des solutions qui, en tout état de cause, méritent d'être évaluées en fonction de la finalité du téléservice public et du degré de sécurité que l'on en attend.

En revanche, le recours à des procédés de chiffrement destinés à assurer la confidentialité des données transmises constitue, pour la CNIL, un impératif dès lors qu'il s'agit de transmettre par des réseaux ouverts de type Internet des informations sensibles telles que des données de santé ou des données financières. La libéralisation, en France, de l'utilisation des moyens de cryptologie a peu à peu permis à la CNIL de préciser, voire de renforcer les exigences qui lui paraissent minimales en la matière[2].

---

1 Ainsi lors de l'avis rendu le 3 février 2000 sur la télédéclaration d'impôt sur le revenu, la CNIL a t-elle demandé que l'administration fiscale étudie un renforcement des dispositifs de sécurité incluant la mise en place d'un procédé de signature électronique (devant d'ailleurs conduire à ce que chaque époux puisse disposer d'une signature électronique). Cette demande a été réaffirmée lors de l'avis du 8 février 2001.

2 C'est ainsi que dans le domaine de la santé, la Commission estime nécessaire de rappeler, dans une recommandation du 4 février 1997 sur le traitement des données de santé à caractère personnel, que les données de santé, confidentielles par nature, devaient surtout si elles sont appelées à circuler sur Internet bénéficier de mesures de protection particulières, leur chiffrement par algorithme de cryptage, constituant

7 — QUEL DOIT ETRE LE DEGRE D'INTERVENTION DU SECTEUR PRIVÉ DANS LE DÉVELOPPEMENT DE L'ADMINISTRATION ÉLECTRONIQUE ?

Les ministres des États membres de l'Union européenne, en novembre 2001, ont exprimé leurs « réserves concernant une dépendance envers un fournisseur unique pour des services de technologies de l'information et de la communication et souhaitaient encourager le développement des logiciels libres, l'interopérabilité des réseaux et des services qui requiert des normes ouvertes et une réglementation technologiquement neutre ».

Est-il envisageable d'envisager un encadrement juridique (national, européen ?) de l'intervention de prestataires privés dans le domaine de l'administration électronique ? Et si oui, selon quelles modalités ?

Ces réflexions et interrogations témoignent de l'importance des enjeux, en termes de protection des données, qui se dessinent avec le développement de l'administration électronique. Même si on constate encore, sinon une relative perplexité du moins une grande prudence de la part de tous, gouvernants, administrations, citoyens, sur les orientations à retenir, aujourd'hui, les offres techniques existent sur le marché, et la pression commerciale est forte en ce domaine. Il apparaît dès lors indispensable que les décisions politiques qui seront adoptées en ce domaine soient prises en pleine connaissance de cause sans forcément épouser les tendances du marché de l'offre technique, au demeurant très évolutives, en tout cas en veillant à ce que l'emploi de telles offres soit justifié par l'intérêt général auquel, évidemment, les enjeux éthiques ne devraient pas demeurer étrangers.

L'ensemble de ces considérations générales incite la Commission à préférer procéder par analyse de projets concrets — fussent-ils à moyen ou long terme — plutôt qu'à embrasser un concept aux contours trop flous dans un monde technologique en profondes et constantes mutations. Cette « dévirtualisation » des débats sur l'administration électronique n'est d'ailleurs nullement un frein à la modernisation de nos administrations au plus grand service des usagers. Elle la sert, comme l'illustre les premières étapes de la mise en place du programme Copernic au sein des administrations financières.

à cet égard, l'une des seules garanties réellement efficaces. Dans le domaine social, La Commission a, dès 1995 lors de l'avis rendu sur la mise en place, par la CNAMTS, du codage des actes de biologie appelés à être télétransmis aux caisses de sécurité sociale par les professionnels de santé, considéré « qu'eu égard aux risques de divulgation et d'utilisation détournée des informations, la CNAMTS devait examiner les modalités qui pourraient être mises en œuvre afin de chiffrer les données d'identification des assurés. Les mêmes observations ont été présentées lors de l'avis du 4 juin 1996 rendu sur le codage des médicaments et la Commission, à l'occasion de la généralisation du dispositif SESAM VITALE a, a nouveau, appelé l'attention des pouvoirs publics sur cette exigence. Actuellement, en effet, seul le code des actes figurant sur les feuilles de soins fait l'objet d'un « brouillage ». Pour des raisons techniques, il est aujourd'hui envisagé que la fonction de chiffrement des informations, qui devait être assurée initialement par la carte, soit de préférence assurée par un dispositif implanté directement sous forme logicielle dans le poste de travail du professionnel de santé. Cette solution n est pas encore opérationnelle. Des solutions de chiffrement ont également été prévues tant en ce qui concerne les télédéclarations sociales (TDS NET) que fiscales (télédéclarations de revenus), la CNIL ayant pris acte que l'assouplissement de la réglementation en matière de cryptologie permettait aujourd'hui de disposer de produits de sécurité sérieux reposant sur des niveaux de chiffrement forts. Enfin, la Commission a estimé, lors de l'avis rendu sur la procédure téléTVA (avis du 12 juin 2001), que de tels disposi ifs devaient être instaurés dès lors que le recours à la téléprocédure revêtait un caractère obligatoire.

B. Une illustration de l'administration électronique : le programme Copernic

Le projet d'administration électronique le plus avancé à ce jour est celui du ministère de l'Economie, des Finances et de l'Industrie (MINEFI), plus particulièrement dans son volet fiscal — le « programme Copernic » — auquel la Commission a consacré plusieurs de ses séances. Compte tenu de son importance, elle a estimé nécessaire d'être régulièrement informée de l'état d'avancement du programme et a, en particulier, entendu en juin 2001 les directeurs généraux des administrations concernées. Ce projet vise une refonte globale des systèmes d'information des administrations fiscales.

1 — UN SYSTÈME DE GESTION INTÉGRÉE DES INFORMATIONS, COMMUN À L'ENSEMBLE DES SERVICES

Outre la poursuite de la dématérialisation des échanges de données fiscales avec les contribuables et ses autres partenaires habituels dans le domaine fiscal (collectivités locales, notaires...), l'objectif du ministère est d'abord de mettre en place un dispositif informatique commun à la direction générale des impôts et à la direction générale de la comptabilité publique destiné à favoriser la circulation de l'information entre leurs services respectifs et entre les applications de gestion de l'assiette, du recouvrement, du contrôle et du contentieux des impôts.

Le programme Copernic, qui n'est pas subordonné à un préalable tenant à une nouvelle organisation des administrations concernées, et qui respecte notamment le principe de la séparation entre ordonnateurs et comptables, s'appuie sur une analyse critique des applications fiscales actuellement utilisées : celles-ci ont, en effet, été conçues à l'origine pour automatiser des processus administratifs préexistants, qui étaient caractérisés par une grande spécialisation des services fiscaux autour d'un « métier » (la gestion de l'assiette, le recouvrement, le contrôle...) et de certains impôts (distinction entre les services de fiscalité personnelle, de fiscalité immobilière et de fiscalité professionnelle). Le recours à l'outil informatique n'a pas été l'occasion de redéfinir l'organisation des services ou de modifier les circuits d'information en vigueur, si bien que la plupart des traitements informatiques existants sont centrés sur les besoins immédiats d'une catégorie de services et non sur les attentes, plus « transversales », des contribuables en matière d'information ou de réactivité de l'administration (par exemple en cas de modification de sa situation ayant une incidence sur plusieurs de ses obligations fiscales). En outre, les applications ont été conçues en « tuyau de cheminée », c'est-à-dire que chacune gère directement la totalité des éléments nécessaires à sa production, en fonction de sa propre logique.

Il s'ensuit un fort cloisonnement des applications et un nombre important de ce que les spécialistes en matière d'organisation appellent des « lignes de fracture structurelles » qui sont autant d'obstacles à la circulation de l'information entre les services fiscaux : segmentation des applications par métier, impôt et zone géographique ; multiplicité des identifiants utilisés, ceux-ci n'étant, en outre, pas pérennes

(l'identifiant fiscal individuel national, le n° SPI, n'est pas généralisé et constitue rarement l'identifiant de base des traitements) ; fréquente duplication des mêmes données dans plusieurs traitements, nécessitant leur saisie à de multiples reprises ; absence de répercussion automatique et simultanée des mises à jour des informations dans les différentes applications (archétype de cette situation, l'adresse est gérée séparément dans huit applications), conduisant à la mise à disposition des services de données d'inégale « fraîcheur » selon les applications. Les mesures ponctuelles adoptées ces dernières années pour tenter de remédier aux défauts les plus notables de cette architecture informatique ne se sont pas révélées être suffisantes : il est toujours difficile aujourd'hui d'avoir une vision globale de la situation fiscale d'un contribuable. Ce diagnostic a conduit l'administration à souhaiter passer d'une logique d'interconnexions plus ou moins régulières entre ses traitements fiscaux à une logique de gestion intégrée de l'ensemble des données, en particulier des données de référence.

2 — « LE CONTRIBUABLE PLACE AU CENTRE DU SYSTEME D'INFORMATION DES ADMINISTRATIONS FISCALES »

L'idée maîtresse du programme Copernic consiste à gérer l'ensemble des informations connues des services fiscaux en fonction de chacune des personnes concernées — personne physique ou entreprise, grâce à la création d'un dossier fiscal informatisé unique, appelé « dossier fiscal simplifié », auquel le contribuable aura accès à travers divers canaux (Internet, bornes interactives, guichet, téléphone) au même titre que les différents services fiscaux amenés à intervenir sur son dossier, sous réserve cependant que les informations mises à sa disposition ne portent pas atteinte à la lutte contre la fraude fiscale. Sur ce point, Copernic s'inspire du projet précurseur GIR de la direction générale de la comptabilité publique et de son interface usagers, dénommé SATELIT, qui avaient été examinés en 2000 par la Commission *[cf.* délibération n° 00-021 du 30 mars 2000) et qui visaient déjà à recourir aux nouvelles technologies de l'information et de la communication pour mettre en place un service de télérèglement de l'impôt et un compte fiscal, unique pour chaque contribuable, consultable par Internet par l'intéressé et regroupant les données relatives au paiement de ses différents impôts.

Une telle orientation suppose, au préalable, de distinguer ce qui se rattache à la personne physique elle-même de ce qui concerne le contribuable au sens strict (le foyer fiscal, l'indivision...) afin de réserver chaque information aux seuls individus qui ont le droit d'en connaître. Ainsi, dans un couple, il arrive qu'une taxe foncière ne soit due que par l'un de ses membres. Lui seul devra avoir accès à cette information, alors que les éléments d'impôt sur le revenu devront être partagés.

A terme, c'est la dématérialisation complète des échanges avec les administrations fiscales que devrait proposer le dossier fiscal simplifié : chaque contribuable aurait la possibilité de consulter son dossier — Copernic facilitera l'exercice du droit d'accès —, de participer à la mise à jour des données le concernant (ex. : notifier ses changements d'adresse), de transmettre ses déclarations, de payer ses impôts ou d'accéder à de nouveaux services (procéder à des simulations, adresser des

demandes de conseils, recevoir des informations personnalisées correspondant à ses besoins, suivre le traitement de ses réclamations...).

3 — UNE GESTION CENTRALISEE, DES ACCES DEMULTIPLIES

Dans sa conception globale, le programme Copernic se caractérise par un mélange de centralisation (en matière de gestion de l'information) et de décentralisation (en matière de diffusion de l'information). Le « projet-cible » prévoit la création de plusieurs bases de données de référence — appelées « référentiels généraux ou transversaux » — qui regrouperont au niveau national l'ensemble des informations communes à tous les services, tous les impôts et tous les « métiers ». Ces informations concernent les personnes — physiques ou morales, particuliers ou professionnels —, les adresses, les services fiscaux, leurs agents et leur domaine de compétence et seront mises à jour de manière centralisée. L'identification des contribuables devrait ainsi être garantie et les actuels doublons (deux identités correspondant en réalité à une même personne) éliminés. Ces bases alimenteront les applications de gestion des données spécialisées où seront conservés les renseignements relatifs aux occurrences fiscales, aux données de recoupement, aux droits de propriété, aux actions administratives ou encore aux parcelles cadastrales.

L'interopérabilité deviendrait ainsi la règle mais serait circonscrite à l'intérieur de la sphère fiscale. Dans ce cadre, les promoteurs du projet souhaitent que l'accès à l'information soit largement ouvert au bénéfice des agents des administrations fiscales grâce à l'Intranet du ministère. En contrepartie, afin d'assurer le respect du secret fiscal et d'éviter toute dérive dans l'utilisation de l'information au sein de l'administration, le ministère s'engage à ce que l'accès aux données soit strictement contrôlé : la gestion des habilitations devra être rigoureuse ; les procédures d'authentification préalable porteront sur les agents utilisateurs et non sur les postes de travail qui peuvent être utilisés par plusieurs personnes ; la traçabilité des consultations sera généralisée ; des contrôles réguliers seront effectués, un outil d'analyse des consultations étant spécialement développé à cette fin.

4 — DES OPERATIONS SOUS COUVERT D'ANONYMAT OU FORTEMENT SÉCURISÉES

Vis-à-vis des contribuables, certains services seront en libre accès. La levée de l'anonymat des internautes consultant le site du ministère n'est prévue que lorsqu'elle s'avère indispensable, ce qui n'est pas le cas lorsqu'un usager souhaite utiliser un outil de simulation ou de calcul de son futur impôt par exemple. De même, la plupart des services de conseil seront accessibles de manière anonyme.

D'autres services, au contraire, ne seront accessibles que sur authentification préalable, avec recours aux technologies les plus modernes, notamment à la signature électronique. Cependant, dans cette hypothèse, le ministère s'engage à établir une stricte séparation entre ses services selon qu'ils rempliront une fonction de conseil ou de contrôle. Le ministère souhaite également, dans la mesure du possible,

laisser toute liberté aux internautes pour utiliser les certificats numériques et adopter les mesures de sécurité de leur choix dans le cadre des téléprocédures fiscales. Les certificats acceptés devront cependant répondre à des critères de sécurité, avec un niveau d'exigence variable selon les services, et de leur degré de sensibilité.

La refondation du système d'information des administrations fiscales sera progressive. Bien qu'il s'agisse d'un programme à long terme — six/sept ans sont prévus pour reconfigurer près de 150 applications —, le plan de mise en œuvre est conçu de telle manière qu'il trouve une traduction concrète dès le court terme, en particulier pour les nouveaux services destinés aux contribuables.

5 — LES PREMIERES ETAPES DU PROGRAMME COPERNIC

Depuis le lancement du programme Copernic, la CNIL s'est déjà prononcée sur trois de ses principaux volets : en mai 2001 sur les téléprocédures relatives à la TVA ; en mars 2002, sur les téléservices proposés aux particuliers en matière de dématérialisation de la déclaration de revenus et de consultation du dossier fiscal simplifié via Internet ; en octobbre 2001 sur la refonte des procédures de transfert de données fiscales aux organismes de sécurité sociale.

TéléTVA est la première téléprocédure sécurisée par l'utilisation de certificats numériques. Ce service permet aux entreprises de télédéclarer et de télérégler la TVA et les taxes assimilées aux taxes sur le chiffre d'affaires, de consulter l'historique de leur situation et d'obtenir en ligne des certificats de dépôt et de paiement valant accusé de réception. Deux solutions techniques sont proposées aux redevables professionnels : l'échange de données informatisées (EDI) et Internet.

Dans la seconde configuration, le dispositif permet de remplir sa déclaration en bénéficiant d'un service d'aide et de contrôle de cohérence, d'y joindre le règlement correspondant, de consulter les déclarations et les règlements déjà transmis ainsi que les avis de réception associés, ou encore de gérer ses certificats numériques en fonction de l'organisation interne de l'entreprise et des délégations de responsabilité.

Les certificats numériques utilisés pour sécuriser les échanges via Internet sont obtenus auprès d'une autorité de certification du marché mais doivent avoir été référencés par le ministère. Cependant, ils ne comportent aucune information spécifique aux applications de l'administration fiscale et pourront donc être utilisés à d'autres fins. En revanche, dans le cas de l'EDI, la direction générale des impôts fait office d'autorité de certification, solution déjà retenue pour la procédure TDFC de transmission des déclarations de résultats. L'utilisation du service TéléTVA est obligatoire pour les entreprises qui relèvent de la direction des grandes entreprises. Dans sa délibération, la Commission s'est notamment prononcée sur le chiffrement des données transmises — qu'elle estime indispensable dès lors que le recours à la téléprocédure a un caractère obligatoire -, sur les modalités d'information des usagers — dont elle a souhaité le renforcement — et sur les conditions à remplir en cas de recours à la sous-traitance.

Délibération n° 01-037 du 12 juin 2001 relative à la mise en place de procédures dématérialisées de déclaration et de règlement en matière de TVA

(Demande d'avis n° 747333)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministre de l'Économie, des Finances et de l'Industrie d'un projet d'arrêté « autorisant la mise en oeuvre à la direction générale des impôts d'un traitement automatisé dénommé TéléTVA, permettant d'effectuer des opérations de transmission par voie électronique des éléments déclaratifs et de paiement de la taxe sur la valeur ajoutée et des taxes assimilées » ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe 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 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ; Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, ensemble le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Vu le code général des impôts, notamment les articles 1649 quater B bis, 1649 ouater B quater et 1695 quater ;

Vu le Livre des procédures fiscales, notamment les articles L. 170, L. 176 et L. 176 A ;

Vu le décret n° 2000-1036 du 23 octobre 2000 pris pour l'application des articles 1649 quater B bis et 1649 quater B quater du code général des impôts et relatif à la transmission des déclarations fiscales professionnelles par voie électronique ;

Vu l'arrêté du 23 octobre 2000 portant convention type relative aux opérations de transfert de données fiscales effectuées par des partenaires de la direction générale des impôts pour les échanges de données informatisés ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ; **Rend l'avis suivant** :

Le dispositif dénommé « TéléTVA » qui est soumis à l'examen de la CNIL par le ministère de l'Economie, des Finances et de l'Industrie (Minefi), a pour finalité de permettre aux contribuables de transmettre par voie électronique à la direction générale des impôts (AGI), notamment par Internet, les éléments déclaratifs et éventuellement de paiement relatifs à la taxe sur la valeur ajoutée et aux taxes assimilées aux taxes sur le chiffre d'affaires.

« TéléTVÀ » regroupe un ensemble de services qui assure l'envoi, dans un même message, de la déclaration et du paiement. L'adhésion à la téléprocédure est proposée :

— aux contribuables qui ont l'obligation de transmettre par voie électro nique leurs déclarations de TVA et les règlements qui leurs sont associés ;

— à tous les contribuables soumis à des obligations déclaratives en matière de TVA qui souhaitent y souscrire volontairement, qu'ils relèvent du régime réel normal, du régime mini réel, du régime simplifié d'imposition ou du ré gime simplifié agricole.

Les documents déclaratifs actuellement susceptibles d'être dématérialisés sont :

— la déclaration mensuelle ou trimestrielle CA 3 et les formulaires annexes, qui sont propres aux régimes réel normal et mini réel ;

— la déclaration annuelle de régularisation relative au régime simplifié d'imposition ;

— la déclaration propre au régime simplifié agricole ;

— la déclaration de régularisation spécifique au régime simplifié agricole.

Le procédé de télépaiement retenu s'appuie sur la procédure de télérèglement de type A, qui suppose une adhésion préalable du contribuable au télérèglement, donnée lors de la souscription à la téléprocédure, puis un ordre de paiement spécifique pour chaque opération, lors de la signature de la télédéclaration et du télépaiement.

Le règlement peut être partiel et son montant ventilé sur trois comptes, selon le souhait du redevable et pour les montants qu'il indique. Le prélèvement n'est effectué qu'à la date limite de paiement. Aucune somme d'argent ne transitant via l'Internet, l'opération peut être réalisée par un expert-comptable dès lors qu'elle consiste seulement dans la transmission des éléments nécessaires au paiement et ne participe en rien à la délivrance des fonds.

Ces modalités générales n'appellent pas d'observations particulières de la part de la Commission.

En ce *qui concerne le « contrat d'adhésion » à la téléprocédure*

Le recours à la procédure dématérialisée est lié au dépôt préalable par le redevable d'un formulaire de souscription à « TéléTVA » auprès de la recette des impôts dont il relève, qu'il soit souscripteur à titre obligatoire ou optionnel. À l'égard de l'adhérent volontaire, ce document tient lieu de contrat au sens de l'article 1649 quater B bis du code général des impôts (CGI). Il doit y indiquer s'il adhère au dispositif pour la seule télédéclaration ou s'il opte également pour le télérèglement.

Le formulaire de souscription renvoie, par ailleurs, à un « cahier des dispositions générales » pour la description des caractéristiques de la procédure fixées par l'administration. Ce document étant indissociable du contrat prévu par la loi, le non-respect de ses clauses serait de nature à engager la responsabilité de l'État.

Le formulaire de souscription comporte notamment une clause par laquelle l'adhérent « autorise le partenaire EDI qu'il a mandaté à avoir recours, à titre de sous-traitance, à un autre partenaire EDI agréé par la DGI ». Cette disposition étant de nature à influer sur les « modalités de transmission » des déclarations qui doivent être définies par arrêté pris après avis de la CNIL, l'article 5 du projet d'arrêté devrait être complété en ce sens.

En outre, le formulaire de souscription et le cahier des dispositions générales — page 11 — devraient être précisés afin de rappeler que le seuil de 100 millions de francs hors taxe de chiffre d'affaires à prendre en considération, au titre des articles 1649 quater B quater et 1695 quater du CGI, pour déli miter le champ de l'obligation de télétransmission s'applique au précédent exercice de l'entreprise, c'est-à-dire celui qui fait l'objet de la dernière décla ration de résultat.

En ce qui concerne les modalités techniques de transmission des informations

« TéléTVA » propose deux modalités techniques de transmission des déclarations de TVA et des paiements associés, qui sont exclusives l'une de l'autre. La sécurité de l'ensemble des échanges est assurée par l'utilisation de la signature électronique qui garantit l'authentification, la non-répudiation de l'émetteur et l'intégrité des données transmises, notamment des comptes bancaires et des montants indiqués par le redevable.

1) La procédure d'échange de données informatisé (EDI) consiste à per mettre le transfert des fichiers d'ordinateur à ordinateur. Le déclarant est invi té à renseigner, à partir de son micro-ordinateur et de son logiciel de gestion, un formulaire préexistant et à l'envoyer à l'administration, via un « réseau téléphonique spécial » (ex. : Numéris) ou sur support magnétique. Les données envoyées sont conformes à la norme EDIFACT qui permet à l'ad ministration, après traitement automatique, de les intégrer directement dans ses systèmes informatiques.

Le « partenaire EDI » de la DGI pour les échanges de données informatisées peut être :

— un organisme-relais choisi par le déclarant pour intervenir en son nom et pour son compte ;

— le contribuable lui-même, s'il a acquis cette qualité, pour son compte per sonnel.

Les relations entre le « partenaire EDI » et l'administration fiscale sont régies par une convention type, dont les termes ont été fixés par arrêté du 23 octobre 2000.

Dans le cadre de l'EDI, la DGI assure elle-même la fonction d'autorité de certification : lors de son agrément, le « partenaire EDI » reçoit de la DGI le certificat qui l'authentifiera. Au préalable, la DGI aura établi et validé les éléments qui identifieront de façon unique ce partenaire, puis les aura signés afin de les rendre infalsifiables.

2) La procédure d'échange de formulaires informatisé (EFI) par Internet met en relation une personne connectée et une machine serveur placée sous le contrôle de la DGI. Elle permet au déclarant de récupérer en ligne, depuis le site Internet du Minefi, un formulaire dématérialisé, de l'ouvrir par son navi gateur Internet, de le remplir grâce à un logiciel d'aide à la saisie qui met en œuvre divers contrôles de cohérence et calculs automatiques, de sauvegar der ses travaux sous forme de brouillon, et d'envoyer à l'administration, via Internet, les seules données validées après les avoir confirmées.

L'utilisation de cette procédure suppose que l'entreprise ait préalablement acquis, auprès d'une autorité de certification du marché, un ou plusieurs certificats numériques d'identification.

Toutefois, ne pourront être acceptées et traitées que les télédéclarations s'appuyant sur un certificat référencé par le Minefi et sur des signatures électroniques et moyens de confidentialité conformes aux normes adoptées par le ministère. Les contribuables peuvent choisir librement leur fournisseur de certificats parmi ceux ayant obtenu leur homologation. En outre, les certificats référencés, qui ne contiennent aucune information spécifique à une application du Minefi, peuvent être utilisés par leur titulaire en tant que « ticket unique » d'accès à l'ensemble des téléprocédures du ministère, de même qu'avec d'autres partenaires.

Ces dispositifs n'appellent pas d'observations particulières.

En ce qui concerne le chiffrement des informations transmises

1) S'agissant de la procédure EFI, l'utilisation du protocole SSL V3 garantit le chiffrement des données transmises durant la session. En outre, le déclarant pourra choisir de chiffrer, de 40 à 128 bits, les informations le concernant avant de les transmettre à l'administration fiscale. La Commission prend acte de ce dispositif.

2) S'agissant de la procédure EDI, la Commission observe que les informations fiscales sont communiquées en clair à la DGI par le partenaire EDI, ce qu'elle avait déjà constaté en 2000 pour la télétransmission des déclarations de résultat.

De manière générale, la Commission estime que toute procédure de télédéclaration revêtant un caractère obligatoire devrait mettre en oeuvre un procédé de chiffrement assurant la confidentialité des données transmises par voie électronique.

À cet égard, la Commission estime qu'un dispositif technique devrait permettre à chaque adhérent à la procédure EDI de choisir le degré de confidentialité dont il souhaite bénéficier — y compris un niveau très élevé — pour le transfert des informations le concernant, ce qui suppose que les serveurs de l'administration fiscale soient en mesure d'accepter tous les niveaux de sécurité.

Toutefois, la Commission observe que deux voies étant offertes aux télédéclarants, dont l'une — l'EFI — garantit la confidentialité des informations transmises, le dispositif de télétransmission mis en place peut être accepté, à la condition que les contribuables soient informés, par une clause appropriée du cahier des dispositions générales, de ce que les informations les concernant sont transmises en clair, dans le cas de la procédure EDI, entre le partenaire EDI et la DGI et que seule la signature électronique fait l'objet d'un procédé de chiffrement qui garantit l'origine et l'intégrité des données, mais non leur confidentialité.

En ce qui concerne les modalités d'exploitation des informations

La DGI se réserve la faculté de confier à un prestataire externe le soin d'assurer la gestion technique des téléprocédures, l'exploitation du serveur « TéléTVA » et la prise en charge des fichiers des télédéclarations et des télérèglements.

La Commission estime que/dans cette hypothèse, les traitements mis en oeuvre par le prestataire doivent être installés dans des environnements sécurisés et entièrement automatisés. En outre, le cahier des dispositions généra-

les et l'article 5 du projet d'arrêté devraient être complétés comme suit : « la direction générale des impôts peut faire appel à un prestataire externe pour la gestion technique des téléprocédures, l'exploitation du serveur "TéléTVA" et la prise en charge des fichiers des télédéclarations et des télérèglements. Dans cette éventualité, les chaînes de traitements mises en œuvre par le prestataire sont entièrement automatisées et installées dans des environnements sécurisés. Le prestataire ne peut faire usage des informations traitées à d'autres fins que celles prévues par le présent arrêté, notamment pour son propre compte. »

En ce qui *concerne les garanties apportées aux adhérents, notamment en cas de dysfonctionnement du système*

Le cahier des dispositions générales précité indique, d'une part, que « le redevable reste tenu au respect de ses obligations fiscales. En cas de défaillance du partenaire EDI, c'est le redevable qui fera l'objet des mises en demeure et, le cas échéant, des suites que prévoit la législation en vigueur » (page 10), d'autre part, que « le souscripteur est responsable des données télédéclarées et téléréglées. Les données transmises sont réputées émaner régulièrement des redevables » (page 12).

La Commission observe que ces clauses ne sauraient faire échec à l'application des règles générales qui gouvernent le droit de la responsabilité, et que la responsabilité de l'adhérent ne pourra être engagée que pour autant qu'il aura été mis en mesure de réagir utilement en cas de défaillance technique et qu'il aura disposé, à cette fin, de toute l'information nécessaire sur le contenu et les suites de chaque transfert électronique le concernant.

1) Il est prévu que l'adhérent EDI reçoive, à ce titre, sur simple appel téléphonique d'un serveur vocal, un avis de réception de dépôt (CED) et un accusé de réception de paiement accompagné d'un numéro POP (certificat de prise en compte de l'ordre de paiement), la confidentialité des données transmises étant garantie par la combinaison d'un code d'accès et d'un mot de passe choisi par le contribuable.

Il convient cependant que des mesures comparables à celles adoptées par l'administration fiscale dans le cadre des procédures « TDFC » de télétransmission des déclarations de résultat soient prises pour réduire le risque de mises en demeure intempestives en cas de dysfonctionnement de la procédure « EDI-Télé TVA », telles que la réduction des délais de mise des télédéclarations à la disposition des services fiscaux, l'aménagement du calendrier des obligations déclaratives en cas d'incident technique, la mise en place d'une structure départementale ayant pour mission d'effectuer, pour chaque incident, un suivi personnalisé et une analyse.

2) S'agissant de la procédure EFI, la délivrance d'un avis de réception du dépôt à la fin de la transaction assure le redevable de la bonne réception par la DGI du fichier transmis. En outre, ce dernier peut obtenir la preuve qu'il a accompli ses obligations déclaratives dans les délais prévus par :

— la délivrance d'un avis de réception du dépôt par le même serveur vocal que pour les adhérent EDI, accessible sur simple appel téléphonique ;

— l'envoi à l'adresse électronique du souscripteur d'un certificat de dépôt CEDP et d'un certificat de paiement CPOP, à l'exclusion de toute transmis sion d'informations confidentielles ;

— la consultation via Internet, à partir d'une transaction sécurisée, de la télédéclaration déposée, de l'accusé de réception du paiement et du numéro CPOP qui atteste de l'envoi de l'ordre de paiement à la Banque de France.

En outre, dans l'hypothèse où le souscripteur aurait des difficultés ou des inquiétudes lors des opérations de transmission des informations le concernant, il dispose d'une assistance téléphonique et peut, en dernier recours, contacter la recette des impôts dont il relève.

Enfin, en cas d'indisponibilité du service, le souscripteur en est averti par un message affiché sur le site du ministère et délivré par l'assistance téléphonique. Dans ce seul cas, il est autorisé, après avoir pris l'attache de sa recette des impôts, à recourir aux procédures traditionnelles d'envoi de déclarations papier et de règlements.

La Commission prend acte de ces mesures, destinées à assurer l'information du contribuable sur l'issue des téléprocédures le concernant.

En ce qui concerne les services annexes proposés aux adhérents

Les adhérents EFI pourront consulter les télédéclarations, les avis de réception de leur dépôt et les télérèglements les concernant pendant les deux années suivants l'année du dépôt, depuis la zone sécurisée du serveur TéléTVA, c'est-à-dire après authentification sur présentation du certificat numérique et sous une connexion chiffrée et sécurisée.

Ils bénéficient également d'une fonction de gestion des certificats numériques qui permet de déléguer à un tiers le pouvoir de télédéclarer et de télérégler.

Par ailleurs, la mise en oeuvre d'une procédure de « rejeu », à la demande de l'administration ou du souscripteur — qu'il ait adhéré à l'EDI ou à l'EFI —, permet de s'assurer de la concordance entre les données transmises par le déclarant ou pour son compte et les données restituées à la DGI. À cette fin, les télédéclarations sont archivées dans le format d'origine produit par l'émetteur. La transmission des éléments ainsi conservés est effectuée par envoi recommandé dans les deux mois suivant la réception de la demande écrite.

La DGI prévoit toutefois, dans le cahier des dispositions générales — page 19 —, que « cette procédure n'est mise en œuvre que dans les cas où le redevable conteste l'existence de la déclaration, ou les éléments de celle-ci, qui lui sont opposées par le service gestionnaire. En conséquence, elle ne concerne pas les cas où la réclamation tend uniquement à la réparation d'erreurs ou d'omissions commises par le déclarant », ni lorsque la réclamation concerne les dates de dépôt.

La Commission rappelle que le droit d'accès, tel qu'il est organisé par la loi du 6 janvier 1978, ne prévoit pas d'autres exceptions que celles prévues à l'article 35 de la loi (demandes répétitives) et que son exercice n'a pas à être justifié. En conséquence, s'il est légitime de préciser dans quelles hypothèses a procédure de « rejeu » est tout particulièrement adaptée, il convient de ne pas exclure de façon générale son emploi dans d'autres circonstances. Les clauses précitées du cahier des dispositions générales devraient être modifiées en ce sens.

En ce qui concerne la durée de conservation des informations

Le projet d'arrêté prévoit que, dans le cadre de la mise en œuvre de la procédure d'archivage « rejeu », les informations sont conservées pendant la période d'exercice du droit de reprise prévu par les articles L. 176 et L. 177 du Livre des procédures fiscales, soit jusqu'au 31 décembre de la quatrième année suivant celle au cours de laquelle la taxe est devenue exigible.

Il ajoute toutefois qu'en tout état de cause, la durée de conservation ne peut excéder dix ans, conformément à l'article L. 170 du même livre. Il est précisé, par ailleurs, que cette durée a été déterminée par analogie avec les règles d'archivage applicables aux documents papier correspondants qui ont été définies en collaboration avec la direction des archives de France.

Or, il ressort de l'examen des dispositions pertinentes du Livre des procédures fiscales que l'article L. 170 ne concerne que les impôts directs d'Etat et que le droit de reprise de l'administration s'exerce au maximum en matière de taxes sur le chiffre d'affaires, selon les articles L. 176 et L. 176 A, jusqu'à la fin de la sixième année suivant l'année d'exigibilité. La durée de conservation globale devrait être fixée en conséquence et l'article 6 du projet d'arrêté modifié sur ce point.

Le projet d'arrêté prévoit également, s'agissant des relations entre les contribuables et les partenaires EDI, que ces derniers ne conservent les données destinées à l'administration au-delà du temps nécessaire à leur transmission et à leur bonne réception par la DGI qu'avec l'accord du contribuable concerné et pour la réalisation d'opérations effectuées à sa demande.

En outre, les informations ne sont conservées sur le serveur « TéléTVA » que jusqu'au terme de la deuxième année civile suivant leur réception.

Les autres dispositions de la demande d'avis et du projet d'arrêté qui lui est annexé n'appellent pas d'observations particulières.

Au bénéfice de ces observations, la Commission émet un avis favorable sur le projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie relatif au traitement « TéléTVA », **sous réserve** :

— que l'article 5 de l'arrêté soit complété par un deuxième alinéa : « Le mandataire choisi par le redevable peut recourir à un sous-traitant, à la condition que ce dernier ait lui-même été agréé par la direction générale des impôts » ;

— que les dispositions suivantes soient ajoutées dans le cahier des dispositions générales et à l'article 5, dans un troisième alinéa : « la direction générale des impôts peut faire appel à un prestataire externe pour la gestion technique des téléprocédures, l'exploitation du serveur « TéléTVA » et la prise en charge des fichiers de télédéclarations et de télérèglements. Dans cette éventualité, les chaînes de traitements mises en oeuvre par le prestataire sont entièrement automatisées et installées dans des environnements sécurisés. Le prestataire ne peut faire usage des informations traitées à d'autres fins que celles prévues par le présent arrêté, notamment pour son propre compte » ;

— que le premier alinéa de l'article 6 soit modifié comme suit : « Dans le cadre de la mise en œuvre possible de la procédure d'archivage rejeu, la durée de conservation des données par la DGI ou par son sous-traitant ne peut excéder six ans à compter de l'année au titre de laquelle la taxe est devenue exigible » ;

— que les clauses du cahier des dispositions générales qui limitent le re cours à la procédure de « rejeu » à l'existence d'un contentieux soient amé nagées afin que ne soit pas exclue toute utilisation de cette fonction dans d'autres hypothèses, ce qui contreviendrait aux articles 34 et 35 de la loi du 6 janvier 1978 sur le droit d'accès ;
— que le formulaire de souscription précise que le seuil de 100 millions de francs hors taxe de chiffre d'affaires à prendre en considération pour délimi ter le champ de l'obligation de télétransmission s'applique au précédent exercice de l'entreprise qui a été l'objet de la dernière déclaration de résul tat et que le cahier des dispositions générales soit modifié — page 11 — en conséquence ;
— que, jusqu'à la mise en place du dispositif de cryptage dont la Commis sion souhaite qu'il intervienne dans les meilleurs délais, les contribuables ad hérents à « TéléTVA » soient clairement informés, par une clause appropriée du cahier des dispositions générales, du choix qui leur est offert entre deux voies de télétransmission des données, l'une — l'EFI — qui autorise le chiffre ment des données fiscales transmises, l'autre — l'EDI — qui provisoirement ne comporte pas un tel dispositif ;
— que des solutions comparables à celles mises en place dans le cadre de la télétransmission des déclarations de résultat soient adoptées, afin de ré duire le risque de mises en demeure intempestives en cas de dysfonctionne ment de la procédure « EDI-TéléTVA ».

En ce qui concerne les téléprocédures relatives à l'impôt sur le revenu, la direction générale des impôts a soumis à la CNIL, ces dernières années, trois projets successifs. Après une première expérimentation en 2000 qui avait fait l'objet de nombreuses critiques de la part de la Commission (cf. délibération n° 00-010 du 3 février 2000), une nouvelle application, qui tenait compte de certaines de ces recommandations, a été mise en place pour 2001. Dans sa délibération n° 01-008 du 8 février 2001, la Commission a pris acte des améliorations du dispositif au sujet de l'identification des télédéclarants, avant de rappeler l'intérêt qu'il y aurait à recourir à la signature électronique et à voir renforcé le niveau de chiffrement des données pendant leur transfert.

Délibération n° 01-008 du 8 février 2001 concernant les modifications apportées pour 2001 par la direction générale des impôts à la procédure de transmission par Internet des déclarations de revenus

(Demande d'avis modificative n° 685909)

La Commission nationale de l'informatique et des libertés ;
Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie d'un projet d'arrêté modifiant l'arrêté du 25 février 2000 autorisant la mise en œuvre par la direction générale des impôts du traitement informatisé de la transmission par voie électronique des éléments déclaratifs en matière d'im pôt sur les revenus et portant conventions types relatives à ces opérations ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe 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 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le code général des impôts, notamment les articles 170-1 bis, 1649 quater B bis et 1649 quater B ter ;

Vu l'arrêté — déjà mentionné — du 25 février 2000 du ministre de l'Économie, des Finances et de l'Industrie ;

Vu la délibération de la CNIL n° 00-010 du 3 février 2000 concernant la mise en place par la direction générale des impôts d'une procédure de transmission par Internet des déclarations d'impôt sur le revenu ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle en son rapport et Monsieur Michel Capcarrère, commissaire adjoint du Gouvernement, en ses observations ; **Rend l'avis suivant** :

La demande d'avis modificative transmise à la Commission par le ministère de l'Economie, des Finances et de l'Industrie concerne la poursuite, par la direction générale des impôts (DGI), en 2001 — et pour cette seule année —, de l'expérimentation d'un traitement dont la finalité est de permettre aux contribuables qui le souhaitent de souscrire directement sur le réseau Internet leur déclaration globale de revenus ainsi que leurs déclarations complémentaires ou annexes.

À l'issue de l'examen du projet initial de mise en place de la « télédéclaration IR », la Commission avait émis un avis favorable. Elle avait, cependant, tenu à en limiter la portée à la mise en œuvre du traitement à titre expérimental et pour la seule année 2000, et l'avait assorti :

— d'un certain nombre d'observations et de recommandations propres à assurer un meilleur agencement du service rendu aux contribuables ;

— de la demande d'un bilan de l'opération ;

— d'une présentation des perspectives d'aménagement visant à obtenir, dès l'année 2001, un renforcement des dispositifs de sécurité et de chiffrement.

Elle avait, en outre, rappelé que seule la mise en place d'un procédé de signature électronique est susceptible de permettre l'identification sans risque d'erreur du (ou des) auteur (s) de la télédéclaration et de manifester son (ou leur) adhésion au contenu des fichiers reçus par l'administration par voie électronique.

Les aménagements apportés cette année par la DGI au système, lequel est reconduit pour l'essentiel, sont destinés à répondre, d'une part, aux principales difficultés rencontrées en 2000 et aux souhaits des internautes — par l'extension du champ d'utilisation de la téléprocédure à l'ensemble des internautes, quel que soit l'environnement de leur micro-ordinateur, et par la mise en place d'une version simplifiée du dispositif pour les déclarations les plus aisées à remplir —, d'autre part, à certaines des préoccupations exprimées par la Commission dans son avis du 3 février 2000.

Pour ce qui est de cette dernière catégorie de modifications, leur objet est de renforcer le dispositif de sécurité de la déclaration par voie électronique par une meilleure identification des internautes et d'améliorer l'information des

télédéclarants grâce à la réorganisation des circuits internes de traitement de l'information.

En premier lieu, la création d'un « numéro télédéclarant », identifiant non signifiant, attribué de manière aléatoire et destiné à être saisi par l'internaute en sus de ses nom, prénoms et du « numéro FIP » du foyer fiscal, est de nature à répondre aux craintes exprimées par la CNIL sur l'absence de confidentialité du « numéro FIP », seul identifiant précédemment utilisé. En effet, alors que le « numéro FIP » apparaît sur diverses catégories d'avis d'imposition communicables aux tiers, le « numéro télédéclarant » ne figurera que sur le seul formulaire préidentifié de la déclaration des revenus qui, en l'état du projet, devra impérativement avoir été reçu par le contribuable pour que ce dernier soit en mesure d'envoyer une télédéclaration.

La Commission comprend qu'il est dans l'intention de la DGI, au cas où aucun changement ne serait apporté sur ce point à la « télédéclaration IR » en 2002, d'attribuer de nouveaux « numéros télédéclarant » l'année prochaine. En effet, dans l'hypothèse inverse, le risque d'utilisation frauduleuse du système, à l'insu des intéressés, ressurgirait puisque le formulaire de la déclaration de revenus est susceptible d'être demandé en cours d'année à certaines catégories de contribuables par des tiers.

En second lieu, la Commission prend acte que l'accélération de la communication à l'application « ILIAD », utilisée par les centres des impôts (CD1) notamment pour la gestion de l'impôt sur le revenu, des informations télétransmises sera utilisée par l'administration pour permettre aux CDI, dans des délais courts, d'accuser réception des déclarations papier qui seraient reçues après une télédéclaration et dont l'effet sera de rendre caducs les renseignements adressés par voie électronique.

La Commission a également examiné les suites qu'il est prévu d'apporter aux autres recommandations qu'elle a formulées dans son précédent avis. S'agissant de son souhait — pris en compte pour la campagne 2000 d'impôt sur le revenu — que, dans l'attente d'une amélioration du dispositif d'authenfification du déclarant et du contenu de la télédéclaration, la DGI donne instruction à ses services d'examiner avec une bienveillance toute particulière les réclamations liées à des difficultés avérées rencontrées lors de l'utilisation de la télédéclaration, il paraît nécessaire que cette mesure soit reconduite, en l'absence de modification substantielle de l'économie du système. En ce qui concerne la mise en place d'un système d'authentification complète des télédéclarants que la Commission avait souhaité effective dès 2001, la DGI précise que ses services informatiques poursuivent leurs travaux sur le contrôle de l'identité des télédéclarants, qui sont liés aux évolutions attendues dans le domaine de la signature électronique et au projet « COPERNIC » de refonte du système d'information fiscale, mené conjointement avec la direction générale de la comptabilité publique.

La Commission rappelle que seule la mise en place d'une télédéclaration assortie de deux signatures électroniques permettrait à l'administration de se conformer à l'exigence d'engagement des deux époux posée par l'article 170-1 bis du code général des impôts.

La Commission regrette également que le ministère, qui envisageait l'année dernière de rehausser prochainement le niveau de chiffrement, n'ait pas été en mesure de mettre en place, dès cette année, un dispositif offrant le choix aux internautes entre deux niveaux de chiffrement — 40 bits ou 128 bits —

afin de tenir compte de la variété des versions de navigateurs actuellement utilisées dans le public, alors que cette mesure aurait été de nature à renforcer très sensiblement la confidentialité des informations transmises, qui sont destinées à être couvertes par le secret fiscal.

Par ailleurs, la Commission rappelle que l'information diffusée aux internautes qui envisagent de mettre en œuvre la déclaration électronique IR devrait pallier les lacunes du système mis en place et, qu'à cette fin, les écrans de la téléprocédure devraient informer clairement les contribuables sur :

— le niveau de chiffrement des données transmises par voie électronique qui est actuellement garanti dans le cadre de la télédéclaration IR ;

— les délais dans lesquels l'administration estime pouvoir faire parvenir par courrier un récépissé aux télédéclarants, afin que ceux-ci puissent, en l'absence de cette pièce, adresser à l'administration une déclaration « papier » ;

— la possibilité d'envoyer, jusqu'à l'expiration du délai de déclaration, une déclaration papier pour remplacer la télédéclaration déjà transmise ;

— la cause du rejet d'une déclaration électronique, lorsque cette cause réside dans l'existence d'une première télétransmission, et les conséquences à en tirer ;

— la faculté de recevoir, sur leur demande, copie des fichiers de déclaration les concernant transmis par voie électronique pendant les deux années suivant l'année de mise en recouvrement ;

— la nécessité, compte tenu des risques de saturation du réseau, de procéder en temps utile à la télédéclaration ;

— l'intérêt pour le contribuable d'éditer sa télédéclaration afin d'en conserver une copie imprimée ;

— l'intérêt pour le télédéclarant de procéder à l'effacement des fichiers adressés aux services fiscaux de la mémoire du micro-ordinateur utilisé pour l'opération, lorsque celui-ci n'en est pas l'unique utilisateur.

La Commission observe que les autres caractéristiques du traitement mis en place en 2000, qui répondaient à ses souhaits ou n'appelaient pas d'observation de sa part, sont reconduites sans modification.

La Commission appelle toutefois l'attention de la DGI sur la nécessité que les termes du contrat d'adhésion consultable sur Internet soient en tous points conformes à ceux qui sont énoncés dans les arrêtés publiés au Journal officiel, notamment des dernières modifications soumises à la CNIL.

En ce qui concerne la forme de l'arrêté portant création du traitement, la Commission fait observer qu'il conviendrait de prendre un nouvel arrêté plutôt que de procéder par modification de l'arrêté du 25 février 2000 relatif à l'expérimentation menée en 2000 qui a épuisé ses effets.

Compte tenu de ce qui précède, la Commission émet un **avis favorable** à la mise en œuvre du traitement pour la durée de la campagne 2001 de l'impôt sur le revenu.

Le présent avis est assorti de la demande de présentation d'un bilan quantitatif et qualitatif sur les conditions de mise en œuvre en 2001 de la télédéclaration et sur l'état d'avancement des travaux visant au renforcement du dispositif de sécurité ainsi que de la demande d'amélioration de l'information des télédéclarants tant à l'écran que par envois postaux des CDI, conformément aux recommandations précitées et à celles de la délibération de la CNIL n° 00-10 du 3 février 2000, lesquelles sont maintenues.

En 2002, l'administration fiscale a proposé un nouveau dispositif de Télédéclaration IR qui, se distinguant substantiellement des premières expérimentations, constitue l'un des volets essentiels du programme Copernic. Il met en œuvre pour la première fois la signature électronique et une architecture à clés publiques dans le cadre d'un téléservice grand public. Compte tenu de la minceur de l'offre du marché pour les particuliers, le choix a été fait par l'administration fiscale de fournir gratuitement en ligne aux particuliers un certificat, après authentification de leur foyer fiscal. Toutefois, l'administration n'exclut pas d'agréer des opérateurs autres qu'elle-même si le marché se développe. Le bouquet de services proposé comprend, outre la transmission de la déclaration de revenus par Internet, l'ouverture d'une procédure de téléconsultation des premiers éléments du compte fiscal simplifié. La téléprocédure est également améliorée en ce qui concerne les conditions initiales d'identification des internautes intéressés — même si aucun face à face n'est organisé au moment de l'attribution du certificat électronique —, l'envoi en ligne et sans délai d'un accusé de réception, le chiffrement des informations pendant leur transmission — qui est porté à 128 bits —, l'amélioration de la rédaction des clauses contractuelles auxquelles les contribuables doivent souscrire avant d'accomplir leur première déclaration électronique — qui fournissent une information satisfaisante sur les obligations de chacune des parties.

Dans sa délibération, la Commission évoque plusieurs questions sensibles, dont certaines ont trouvé leur solution après discussion avec l'administration : le traitement des informations relatives au nom des organismes bénéficiaires de dons ouvrant droit à déduction fiscale, qui sont susceptibles de relever de l'article 31 de la loi du 6 janvier 1978 — au sujet desquelles l'administration a accepté qu'elles soient effacées de la base de consultation *au bout* de six mois —, l'absence de double signature des déclarations en cas d'imposition commune — cette solution imposée par les textes en vigueur supposerait notamment que les certificats délivrés soient réellement individuels et non plus fondés sur des informations partagées au sein du foyer fiscal —, le risque de « fracture numérique » — si les nouveaux services ne sont pas à court terme proposés aux contribuables non internautes — et l'étendue des profils de consultation de la base définis pour les agents des administrations fiscales — ceux-ci n'ayant été admis par la Commission qu'au prix de la réaffirmation d'une grande exigence dans l'application des contrôles a posteriori prévus par ailleurs.

Délibération n° 02-010 du 7 mars 2002 concernant (a mise à la disposition des particuliers et des agents des administrations fiscales d'un service de consultation des dossiers fiscaux en ligne et la pérennisation de la procédure de transmission par Internet des déclarations annuelles de revenus

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie :

— d'un projet d'arrêté portant création, par la direction générale des impôts, du traitement automatisé de la transmission, par voie électronique, des

éléments déclaratifs en matière d'impôt sur les revenus et portant conventions types relatives à ces opérations ;
— d'un projet d'arrêté portant création par la direction générale des im pôts du traitement automatisé dénommé « Accès au dossier fiscal des parti culiers ADONIS » ;
— de quatre projets d'arrêtés modificatifs modifiant respectivement les arrê tés du 25 juillet 1988 relatif à l'informatisation des inspections d'assiette et de documentation (traitement « ILIAD »), du 5 janvier 1990 relatif au traite ment d'impôt sur le revenu (« IR »), du 5 janvier 1990 relatif au système de gestion de l'identité et des adresses des contribuables (« FIP ») et du 8 mars 1996 régissant le traitement de la taxe d'habitation (« TH »).

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe 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 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 31, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le code général des impôts, notamment les articles 170-1 bis, 200 nouveau, 1649 quater B bis et 1649 quater B ter ;

Vu la délibération n° 01-008 du 8 février 2001 concernant les modifications apportées en 2001 par la Direction générale des impôts à la procédure, mise en place à titre provisoire, de transmission par Internet des déclarations de revenus ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur le projet d'arrêté portant création d'un dispositif de transmission par voie électronique des éléments déclaratifs en matière d'impôt sur le revenu

Ce nouveau traitement a pour objet de pérenniser la possibilité proposée par l'administration aux contribuables depuis l'an 2000 de déclarer leurs revenus via Internet.

Sa mise en œuvre repose sur l'adhésion du déclarant aux clauses d'un contrat type qui définissent les conditions dans lesquelles sont garanties l'identification de l'auteur de l'acte ainsi que l'intégrité, la confidentialité, l'opposabilité et la conservation de chaque transmission. Il énumère notamment les engagements pris par l'administration à ces différents titres.

En ce qui concerne la délivrance du certificat électronique et l'identification du contribuable

Se distinguant fortement des expérimentations menées précédemment par la Direction générale des impôts (DGI), le dispositif prévu comporte la mise en œuvre d'une signature électronique dans le cadre d'une architecture à clés asymétriques. Pour recevoir un certificat électronique, le contribuable s'identifie préalablement en transmettant plusieurs données à caractère personnel qui figurent sur l'exemplaire papier de sa déclaration de revenus reçu pour l'année en cours ou sur le dernier avis d'imposition établi à son nom au titre de l'année précédente.

Un couple de clés est directement généré sur le poste du contribuable au moment où celui-ci s'identifie dans les conditions précitées. La clé privée du contribuable reste placée sous sa responsabilité et ne peut être utilisée qu'assortie d'un mot de passe choisi par lui.

Sa clé publique est transmise à la DGI qui, intervenant en qualité d'autorité d'enregistrement et de certification, l'authentifie à l'aide de sa propre clé privée. Le certificat électronique du contribuable est créé et lui est délivré en ligne, sans délai et gratuitement. Il permettra, à l'exclusion de toute autre utilisation, à l'administration des impôts de vérifier la signature des déclarations de revenus et à son détenteur de s'identifier dans le cadre du service de consultation du dossier fiscal par Internet.

La Commission constate que l'ensemble du dispositif assure le niveau élevé de fiabilité des procédures de télédéclaration qui avait été souhaité par elle.

Elle estime cependant que cette procédure serait encore mieux sécurisée si l'attention des usagers était spécialement appelée sur la nécessité pour eux de préserver la confidentialité de l'un au moins des éléments à caractère personnel utilisés lors de la phase d'identification préalable du contribuable.

Cet élément d'identification dont il conviendrait de préserver spécialement la confidentialité, semble devoir être le « numéro de télédéclarant » qui, d'ores et déjà, est changé chaque année et ne figure que sur l'exemplaire papier du formulaire de déclaration de revenus de l'année. À cet effet, une mention pourrait faire apparaître qu'en cas de communication de ce document à un tiers, le numéro de télédéclarant devra être occulté.

Dans le cas de contribuables faisant l'objet d'une imposition commune, chacun d'eux peut demander à utiliser les téléservices et à recevoir un certificat électronique.

Le contrat auquel adhère le contribuable précise que la signature électronique, associée au certificat, emporte les mêmes conséquences qu'une signature manuscrite du document papier correspondant.

En ce *qui concerne les informations télétransmises, leur collecte et leur communication*

Peuvent être transmises par voie électronique la déclaration d'ensemble des revenus ainsi que les déclarations annexes, après pré-affichage à l'écran des éléments inscrits sur la déclaration papier. En cas de souscription d'une nouvelle déclaration, sur Internet ou sur support papier, celle-ci est considérée comme déclaration rectificative. Ainsi, le contribuable n'est jamais obligé de recourir à la voie électronique pour faire parvenir sa déclaration.

En ce qui concerne les contribuables qui font l'objet d'une imposition commune (pour 2002, il s'agit des seuls couples mariés), la Commission rappelle une nouvelle fois que l'article 170-1 bis du code général des impôts dispose que « les époux doivent conjointement signer la déclaration d'ensemble des revenus de leur foyer. » En conséquence, seule la mise en place d'une télédéclaration assortie de deux signatures électroniques permettrait à l'administration de se conformer à l'exigence d'engagement des deux époux et ainsi de respecter les dispositions légales.

La Commission souhaite que les réflexions en cours sur ce point aboutissent rapidement et prend acte des engagements pris par l'administration sur ce sujet. Elle souhaite qu'une solution soit trouvée en 2003 au plus tard. Afin d'assurer la confidentialité des informations transmises par voie électronique et d'éviter toute utilisation détournée de celles-ci, l'administration s'engage à ce que la totalité des transferts d'informations vers son serveur, lors des phases de saisie de la déclaration et d'envoi de la déclaration signée, s'effectue en mode sécurisé et chiffré (protocole SSLv3, clé de chiffrement de 128 bits).

Après vérification que les fichiers transmis ont été correctement reçus et que la signature électronique de la déclaration correspond à celle du déclarant, l'administration délivre en ligne, sans délai, un accusé de réception comportant notamment les éléments d'identification du contribuable, les date et heure de réception de la déclaration (heure de Paris), le numéro d'accusé de réception ainsi que la liste des documents reçus et acceptés. L'accusé de réception peut être imprimé ou téléchargé, son numéro étant nécessaire en cas de contestation ultérieur du dépôt.

En cas de non-conformité de la déclaration électronique, le contribuable est informé de l'échec de la transmission et invité à déposer une nouvelle déclaration sous forme papier ou dématérialisée.

Outre les informations portées sur les déclarations d'ensemble des revenus et relatives à l'identification des membres du foyer fiscal, à leurs revenus et à leurs charges qui sont habituellement enregistrées en mémoire informatique dans les centres des impôts, la « Télédéclaration IR » prévoit le recueil et la conservation sur support informatique d'informations complémentaires :

— les données portées sur les déclarations annexées à la déclaration d'en semble en présence de certaines catégories de revenus ;

— pendant quinze jours, les données figurant sur les déclarations en cours de saisie ;

— les données littérales de la déclaration d'ensemble, telles que les référen ces des établissements scolaires ou universitaires fréquentés par les enfants à charge et leur niveau d'études, le détail des frais réels ou les nom et adresse des tiers (ex. : salariés employés à domicile, assistantes maternelles, bénéficiaires de pensions alimentaires, entrepreneurs) bénéficiaires de ver sements déclarés au titre des charges ;

— les données littérales ajoutées sur la déclaration électronique en contre partie de la suppression de certaines pièces justificatives : nom des organis mes bénéficiaires de dons, legs ou cotisations ouvrant droit à réduction d'impôt — à l'exception de ceux des organisations syndicales, des associa tions cultuelles ou de bienfaisance et, lorsque leur montant est inférieur ou égal à 3 000 euros, des associations de financement électoral, partis et groupements politiques —, montant total des versements effectués à chacun d'entre eux.

La Commission constate qu'en dépit des précautions prises par le législateur, il ne peut être exclu que le nom des organismes bénéficiaires de dons fasse apparaître indirectement notamment les opinions politiques, philosophiques ou religieuses des contribuables et qu'ainsi il constitue une information dont l'enregistrement et la conservation ne sont normalement envisagés, en application de l'article 31 de la loi du 6 janvier 1978, qu'avec l'accord exprès de l'intéressé ou, pour des motifs d'intérêt public, par décret en Conseil d'État pris sur proposition ou avis conforme de la CNIL.

Toutefois, la Commission considère qu'un tel décret n'est pas nécessaire dès lors que :
— s'agissant de la collecte et de l'enregistrement des informations en cause, le décret ne pourrait que reprendre les termes de la loi ;
— s'agissant des modalités de leur conservation et de leur utilisation, le pro jet d'arrêté relatif au traitement « ADONIS » prévoit, à l'issue de l'instruction du dossier, que ces informations ne sont pas conservées dans « ADONIS » au-delà de six mois — c'est-à-dire le temps nécessaire pour permettre à l'ad ministration d'atteindre l'objectif voulu par le législateur — et que tout traite ment spécifique à partir de ces données est rendu techniquement impossible.

En ce qui concerne la conservation des informations transmises

Afin de garantir l'opposabilité des données reçues par la DGI, l'ensemble des informations transmises (déclarations de revenus signées avec leurs annexes, date et heure des dépôts, données relatives à la certification des envois) sont conservées, chiffrées et signées, pendant dix ans à compter de l'année d'imposition dans une base d'archivage afin de permettre, en cas de contestation du contribuable, la vérification de la signature et du contenu d'une transmission. Ces informations, qui sont intangibles, sont opposables au contribuable et à l'administration. Leur vérification peut être effectuée devant un expert nommé par les tribunaux.

Sur le projet d'arrêté portant création de la base nationale de consultation « ADONIS »

Ce traitement a pour objet principal la mise en place d'un service de consultation en ligne des dossiers nominatifs de fiscalité personnelle des contribuables.

En ce qui concerne le contenu de la base

« ADONIS » comporte, pour chaque foyer fiscal :
— les déclarations d'ensemble des revenus et les déclarations annexes transmises par voie électronique, les date et heure du dépôt des déclara tions, le numéro des accusés de réception électroniques ;
— les éléments des déclarations d'ensemble des revenus reçues sur support papier, lorsqu'ils sont conservés sur support informatique par l'administra tion ;
— les avis d'imposition concernant l'impôt sur le revenu, les contributions sociales (CSG, CRDS), la taxé d'habitation et les taxes foncières ;
— une présentation synthétique du dossier fiscal du contribuable et un résu mé de chaque imposition ;

— des informations relatives aux réclamations, aux impositions supplémentaires émises ainsi qu'aux dégrèvements.

Ces informations sont mises à la disposition de l'ensemble des utilisateurs d'ADONIS dans les mêmes conditions et pendant les mêmes durées de conservation, sous réserve des précisions ci-après.

En ce qui concerne la consultation de la base par les contribuables

Pour avoir accès, via Internet, à son dossier fiscal mis en ligne, chaque contribuable s'authentifie en transmettant le certificat électronique en cours de validité qui lui a été précédemment délivré par la DGI ou dont il obtient la délivrance en suivant la procédure d'identification préalable prévue pour la télédéclaration des revenus. Il ne peut accéder qu'aux informations conservées dans son dossier fiscal.

L'administration met en œuvre un cryptage des données téléconsultées suivant le protocole SSLv3 (clé de chiffrement de 128 bits).

La Commission constate que ce dispositif assure un niveau de sécurisation du téléservice de consultation du dossier fiscal qui, en l'état actuel de la technologie, peut être jugé satisfaisant.

Par ailleurs, la Commission attire l'attention de l'administration sur les dispositions de l'article 35 de la loi du 6 janvier 1978 et sur les termes de sa délibération n° 80-10 du 1er avril 1980 qui impliquent que toutes les informations conservées dans la base, et donc consultables par les contribuables, puissent l'être sous une forme directement compréhensible par eux et donc non codée.

Enfin, la Commission rappelle que le ministère de l'Économie, des Finances et de l'Industrie prévoit de mettre en place, à terme, d'autres dispositifs de consultation des mêmes informations (serveur vocal, bornes publiques de consultation du site du ministère...) afin d'éviter toute « fracture numérique » dans la société. Elle exprime le souhait que ces services soient développés dans les meilleurs délais.

En ce qui concerne la consultation de la base par les agents des administrations fiscales

La consultation de la base « ADONIS » sera en principe ouverte, via l'Intranet ministériel, à tous les agents de la DGI et de la Direction générale de la comptabilité publique (DGCP), sous réserve que ces agents aient à l'égard des contribuables dont les dossiers sont consultés une mission d'assiette, de contrôle ou de recouvrement en matière fiscale.

D'une part, un contrôle a *priori* des accès au traitement est mis en œuvre par l'intermédiaire d'un annuaire qui recense non pas des habilitations individuelles, fonction des attributions géographiques et fonctionnelles précises des agents, mais de « profils applicatifs » plus larges, à caractère géographique. Trois niveaux d'accès à « ADONIS » sont ainsi prévus :

— un niveau national, pour des agents ayant une compétence nationale (bureaux d'administration centrale, directions nationales à compétence spécialisée) et certains agents des directions des services fiscaux et des trésoreries générales ;

— un niveau interrégional, pour certains agents des directions du contrôle fiscal et des trésoreries générales ;

— un niveau départemental pour les autres agents habilités des services déconcentrés de la DGI et de la DGCP (ex. : centres des impôts, trésoreries), étant entendu qu'un agent accède à l'ensemble des données contenues dans les dossiers fiscaux qui comportent au moins une occurrence fiscale située dans son département d'exercice.

En outre, certains dossiers, qualifiés de sensibles par l'administration, feront l'objet d'une protection renforcée de leur confidentialité : seuls quelques agents bénéficiant d'une habilitation supérieure pourront y accéder.

D'autre part, un contrôle *a posteriori* de la bonne application de la règle de consultation est permis grâce à un dispositif de journalisation des consultations par les agents des dossiers fiscaux et de conservation des données correspondantes pendant un an.

La Commission prend acte de ce dispositif. Elle estime qu'ainsi conçu, il n'assurera la nécessaire protection des données à caractère personnel et du secret fiscal qu'au prix d'une grande exigence dans l'application des contrôles a *posteriori* qui sont envisagés.

À cet égard, la Commission estime qu'il serait utile de prévoir un contrôle a *posteriori* aléatoire qui devrait concerner au moins 1 % des interrogations de la base « ADONIS ».

En ce *qui concerne l'utilisation des informations contenues dans la base*

La DGI souhaite être autorisée à utiliser les informations d'identification des contribuables pour mener des enquêtes-qualité sur les téléprocédures fiscales. Elle reconnaît cependant aux intéressés le droit de s'opposer à faire l'objet de ces sollicitations, en application de l'article 26 de la loi du 6 janvier 1978.

La Commission estime qu'indépendamment de l'information assurée par l'arrêté portant création du traitement « ADONIS », il convient que les usagers de ce traitement soient informés du droit d'opposition qui leur est reconnu selon des modalités qui en facilitent l'exercice.

Au bénéfice des observations qui précèdent, la Commission émet un **avis favorable** sur les projets d'arrêtés qui lui sont présentés par le ministère de l'Économie, des Finances et de l'Industrie.

Le présent avis est assorti de la demande de présentation d'un bilan quantitatif et qualitatif sur les conditions de mise en oeuvre en 2002 de ces traitements.

Autre volet du programme Copernic examiné par la CNIL, la procédure TDF vise à améliorer l'accès de certains tiers à l'information fiscale, et plus précisément à refondre dans un système unique les dispositifs existants de transfert de données fiscales en réponse aux demandes que présentent les organismes de Sécurité sociale. Elle trouve son fondement dans la loi de finances pour 1999 et ses décrets d'application qui ont réorganisé le régime des dérogations au secret fiscal dont bénéficient les organismes de protection sociale en établissant la liste des finalités qui, seules, peuvent justifier la transmission d'informations fiscales, en autorisant le recours au numéro d'inscription au répertoire national des personnes physiques tenu par l'INSEE (NIR) pour la réalisation de ces transferts et en définissant les règles auxquelles ils devront satisfaire. Le dispositif respecte les orientations fixées en 1999 pour

l'utilisation du NIR par les administrations fiscales[12]: celui-ci reste confiné dans des fichiers, à finalité purement technique, qui établissent un lien fixe entre le numéro de l'INSEE et l'identifiant fiscal personnel, dénommé n° SPI, qui est attribué par la Direction générale des impôts à toute personne physique ayant la qualité de contribuable. Ces « tables de correspondance » sont conservées dans deux centres informatiques sur des supports dédiés. Elles font l'objet de mesures de sécurité renforcées et ne sont accessibles qu'aux seuls agents chargés de leur maintenance. Au cours de l'instruction du dossier, la Commission s'est efforcée de faire préciser, dans les textes qui lui étaient soumis, les finalités de chaque transfert, la liste détaillée des catégories d'informations transmises, les modalités de l'utilisation par chaque organisme destinataire des données fiscales ainsi que les conditions dans lesquelles ces dernières sont opposables aux personnes concernées.

La délibération de la CNIL qui expose les grandes lignes du nouveau dispositif comporte plusieurs préconisations : les fichiers de demandes d'informations constitués aux fins du contrôle des revenus des bénéficiaires de prestations versées sous condition de ressources ne devraient pas comporter de demandes visant d'autres personnes dont les ressources n'ont pas à être contrôlées, ce que ne permet pas le calendrier des opérations actuellement envisagé. Les NIR utilisés dans la procédure devraient systématiquement avoir été vérifiés auprès de l'INSEE. L'information portée à la connaissance des personnes concernées devrait, dans certains cas, être améliorée. Les fichiers transmis devraient systématiquement être chiffrés.

Par ailleurs, la Commission a rappelé, comme elle avait déjà eu l'occasion de l'exprimer lors de l'examen des précédents dispositifs de transfert de données fiscales à des organismes de Sécurité sociale, qu'elle était favorable à la fusion en une déclaration unique, à la fois fiscale et sociale, des obligations déclaratives en vigueur qui conduisent l'administration fiscale d'une part, les organismes gestionnaires des prestations familiales et les caisses d'assurance maladie des travailleurs indépendants d'autre part, à demander aux mêmes personnes de fournir des éléments similaires sur leurs revenus. Cette solution présenterait, en effet, le double avantage de limiter les transferts de fichiers et d'alléger les obligations administratives à la charge des particuliers.

Délibération n° 01-055 du 25 octobre 2001 relative à la création d'une procédure de transfert de données fiscales pour le compte de l'État et des organismes de protection sociale visés à l'article L. 152 du Livre des procédures fiscales

La Commission nationale de l'informatique et des libertés ;
Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie :
— d'un projet de décret « portant création d'une procédure de transfert des données fiscales » (« TDF ») ;

1 Cf. 20* rapport d'activité pour 1999, p. 66 et suivantes.

— d'un premier projet d'arrêté interministériel « relatif à la mise en service à la direction générale des impôts, à la Caisse nationale d'assurance vieillesse des travailleurs salariés, à la Caisse nationale d'allocations familiales et à la caisse nationale d'assurance maladie des professions indépendantes d'une procédure automatisé de transfert des données fiscales » ;
— d'un second projet d'arrêté interministériel « relatif à la mise en service à la direction générale des impôts et dans les organismes de mutualité sociale agricole d'une procédure automatisée de transfert des données fiscales » ;
— d'un projet de convention « relative au fonctionnement de la procédure TDF » ;

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

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le Livre des procédures fiscales, notamment ses articles L. 152, L. 288, R.* 152, R.* 287 et R.* 288-1 et suivants ;

Vu le code de la sécurité sociale, notamment ses articles L. 542-6, L. 583-3, L. 831-7, L. 843-1, R. 115-5 et R. 652-14 ;

Vu le code de la construction et de l'habitat, notamment son article L. 351-12;

Vu le décret n° 99-1047 du 14 décembre 1999 pris pour l'application de l'article 107 de la loi de finances pour 1999 (n° 98-1266 du 30 décembre 1998) relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects ;

Vu le décret n° 2000-8 du 4 janvier 2000 pris pour l'application de l'article L 288 du Livre des procédures fiscales ;

Après avoir entendu Messieurs Jean-Pierre de Longevialle et Maurice Viennois en leur rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations,

Rend l'avis suivant :

Aux termes de l'article L. 152 du Livre des procédures fiscales (LPF), tel qu'il résulte du IV de l'article 107 de la loi de finances pour 1999 : « les agents des administrations fiscales communiquent aux organismes et services chargés de la gestion d'un régime obligatoire de sécurité sociale et aux institutions mentionnées au chapitre I^{er} du titre II du Livre IX du code de la Sécurité sociale [les institutions gestionnaires d'un régime de retraite complémentaire obligatoire] les informations nominatives nécessaires : « 1) à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations ; « 2) Au calcul des prestations ;

« 3) à l'appréciation des conditions d'assujettissement aux cotisations et contributions ;
« 4) à la détermination de l'assiette et du montant des cotisations et contributions ainsi qu'à leur recouvrement.

« Le numéro d'inscription au répertoire national d'identification des personnes physiques [NIR] est utilisé pour les demandes, échanges et traitements nécessaires à la communication des informations mentionnées au premier alinéa, lorsqu'elles concernent des personnes physiques. »

Par sa décision n° 98-0405 DC du 29 décembre 1998, le Conseil constitutionnel a déclaré que les dispositions issues du IV de l'article 107 susvisé sont conformes à la Constitution, compte tenu de ce que notamment « ces communications doivent être strictement nécessaires et exclusivement destinées à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de l'assiette et du montant des cotisations et contributions, ainsi qu'à leur recouvrement » et de ce que la méconnaissance de ces dispositions sera réprimée dans les conditions prévues par l'article 226-21 du code pénal. Le décret n° 99-1047 du 14 décembre 1999, pris après avis de la CNIL, confirme, au premier alinéa de l'article R.* 152-1 nouveau, que les informations nominatives communiquées par les administrations fiscales « sont limitées à ceux des éléments de la situation fiscale des personnes concernées qui sont strictement nécessaires à l'accomplissement par l'organisme demandeur de sa mission légale ».

Le même décret prévoit que « des arrêtés conjoints des ministres chargés du Budget et, selon le cas, de la Sécurité sociale ou de l'Agriculture pris après avis de la CNIL fixent, pour chaque catégorie d'organismes mentionnés à l'article R.* 152 du LPF », la liste des informations nominatives susceptibles d'être transmises, « les règles auxquelles doivent satisfaire les traitements automatisés opérés pour le recueil et l'exploitation » des informations fiscales, ainsi que « les délais dans lesquels les responsables des traitements déjà mis en œuvre doivent justifier auprès de la [CNIL] que ces traitements sont ou ont été rendus conformes à ces règles ».

Sur le projet de décret

Le projet de décret transmis à la CNIL pour avis institue une procédure unique de transfert automatisé de données fiscales, dénommée « TDF », qui est mise en œuvre pour le compte de l'État et des organismes et services visés à l'article L. 152 du LPF et dont l'objet est de permettre la communication sur support informatique des « informations fiscales nécessaires à l'exécution des finalités décrites à l'article L. 152, dans le cadre de leurs missions légales et dans le respect des dispositions de l'article R.* 152 ».

La procédure est mise en oeuvre dans le cadre d'un centre serveur unique, « hébergé par la direction générale des impôts » (DGI) et dénommé « Centre national de transfert de données fiscales » (CNTDF), qui reçoit les demandes des organismes sociaux participant à la procédure automatisée, les transmet à la DGI et adresse les réponses reçues de celle-ci.

Un comité de gestion du CNTDF, composé d'un représentant de chacun des partenaires au sein de « TDF », est notamment chargé de s'assurer de la mise en place du centre serveur unique, de prendre les mesures nécessaires

à l'application des textes régissant « TDF », de veiller au respect des procédures retenues pour le traitement et le transfert des données, de se prononcer sur l'adhésion de nouveaux partenaires, d'examiner et de statuer sur les incidents de gestion.

Il est précisé que les règles d'ordre technique, fonctionnel, structurel et financier qui sont applicables à « TDF » sont définies par une convention signée par l'ensemble des partenaires de la procédure.

Enfin, l'article 2 dispose, au premier alinéa, que la DGI « est chargée, en liaison avec les organismes [participant à « TDF »] de garantir la confidentialité et la sécurité des traitements et des données et de veiller au bon fonctionnement de la procédure », et à l'alinéa 2, qu'aucun accès aux informations conservées ou transitant par le CNTDF n'est possible auprès de ce dernier et que ces informations demeurent « sous la responsabilité » du partenaire maître du fichier.

La Commission :

— constatant que le document intitulé « projet de convention relative au fonctionnement de la procédure TDF » est incomplet, demande à avoir connaissance de sa version définitive ;

— estime que la rédaction de l'article 2 devrait être clarifiée par l'affirmation qu'il incombe à la direction générale des impôts d'assurer — au lieu de garantir — la confidentialité et la sécurité des traitements mis en œuvre par le CNTDF et des données ainsi traitées et en ne maintenant pas, au second alinéa, la référence à la responsabilité assumée par ailleurs par chaque partenaire vis-à-vis des informations issues de ses propres traitements.

Sur les projets d'arrêtés

En ce qui concerne les organismes destinataires des informations fiscales, les finalités de leur traitement et les conditions de leur exploitation

Les arrêtés présentés à la Commission énumèrent les organismes qui sont autorisés à bénéficier de la procédure « TDF » — la Caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS), la Caisse nationale d'allocations familiales (CNAF), la Caisse nationale d'assurance maladie des professions indépendantes (CANAM) et la Caisse centrale de mutualité sociale agricole (CCMSA) —, définissent les finalités des transferts d'informations fiscales correspondants et décrivent les caractéristiques des traitements automatisés opérés pour l'exploitation de ces informations.

— Pour les informations fiscales relatives aux personnes relevant du régime général des allocations familiales

Ces informations sont exclusivement utilisées par les caisses d'allocations familiales (CAF) pour engager une procédure de contrôle a *posteriori* des ressources des ménages qui bénéficient pendant l'année N, sur la base de leurs ressources de l'année N -1, d'une ou plusieurs des prestations servies sous condition de ressources citées ci-après : l'aide personnalisée au logement (APL), l'allocation logement à caractère social (ALS), l'allocation logement à caractère familial (ALF), la prime de déménagement, l'allocation aux adultes handicapés (AAH), le complément familial, l'allocation pour jeune enfant (APJE), l'allocation d'adoption, l'allocation de rentrée scolaire (ARS), l'allo-

cation de garde d'enfant à domicile (AGED) et l'aide de la famille pour l'emploi d'une assistante maternelle agréée (AFEAMA).

Les informations fiscales servent d'ores et déjà, sur le fondement de précédentes autorisations, à vérifier les déclarations annuelles de ressources transmises par les allocataires qui demandent à percevoir une ou plusieurs de ces prestations. Seules sont prises en compte les divergences entre la déclaration de l'allocataire et les éléments transmis par l'administration fiscale qui sont susceptibles de remettre en cause le montant des prestations en cours de versement.

Lorsque les informations à comparer portent sur des revenus de nature différente — montants bruts déclarés à la DGI, montants nets connus de la CAF — ou lorsque les divergences de montants de ressources globales sont très importantes, un courrier est adressé à l'allocataire qui l'informe de sa situation et lui demande de produire des pièces justificatives.

Dans les autres cas, les informations transmises par la DGI sont substituées à celles déclarées par l'allocataire à sa caisse de rattachement. L'allocataire est alors informé du rappel — lorsque la source fiscale indique des ressources inférieures à celles portées sur la déclaration CAF — ou de l'indu, des voies de recours ainsi que des modalités de recouvrement des sommes à reverser — lorsque les revenus transmis par la DGI sont supérieurs à ceux mentionnés sur la déclaration CAF.

— Pour les informations relatives aux personnes relevant du régime agricole des allocations familiales

Les organismes de Mutualité sociale agricole prévoient également de vérifier, sur la base des informations fiscales, les déclarations relatives aux ressources de l'année N -1 adressées par leurs allocataires qui perçoivent pour l'année N une ou plusieurs des prestations précédemment énumérées.

Un courrier est adressé à l'allocataire lorsque les informations à comparer portent sur des revenus de nature différente. En outre, en présence de divergences faisant supposer l'existence de prestations indues à reverser, une lettre motivée est transmise à l'intéressé qui dispose d'un délai d'un mois pour présenter ses observations et fournir les pièces nécessaires à la justification de sa déclaration.

— Pour les informations relatives aux personnes relevant du régime général ou du régime agricole de l'assurance vieillesse

Ces informations, qui sont transmises aux caisses gestionnaires relevant de la CNAVTS ou de la CCMSA, sont exclusivement utilisées pour déterminer les taux de prélèvement à appliquer sur les pensions de retraites ou d'invalidité du régime général ou du régime agricole de sécurité sociale au titre des contributions et cotisations sociales.

La procédure « TDF » se substitue ainsi aux obligations de déclaration ou de production de pièces précédemment mises à la charge des pensionnés.

— Pour les informations relatives aux personnes relevant du régime d'assurance maladie des travailleurs indépendants (régime CANAM)

Les caisses maladie régionales (CMR) utilisent exclusivement les informations fiscales pour contrôler *a posteriori* les déclarations communes de revenus des assurés sociaux qui servent notamment au calcul de l'assiette des cotisations d'assurance maladie et des contributions sociales.

À l'issue du rapprochement automatisé, dans les centres informatiques de la CANAM, des données fiscales avec le contenu des déclarations communes de revenus des professions indépendantes, seules sont transmises aux CMR des listes relatives aux discordances relevées, où sont portés le résultat du calcul des cotisations dues sur la base des informations de la DGI et l'écart constaté entre l'assiette déclarée et l'assiette ainsi reconstituée.

Des courriers sont adressés aux assurés sociaux cités sur ces listes. Ils mentionnent l'écart constaté entre les deux sources et en demandent la justification. À l'issue de la procédure contradictoire définie à l'article R. 652-14 du code de la Sécurité sociale, seules les rectifications d'assiette sont intégrées dans l'application « SAGA » de la CMR de rattachement.

La Commission constate que les finalités des traitements mis en œuvre sont conformes aux objectifs assignés par la loi à la communication des informations fiscales par la DGI dans le cadre de la procédure « TDF » et pour l'exploitation des informations nominatives ainsi transférées. La Commission estime, par ailleurs, que les précisions ci-dessus indiquées relatives à l'exploitation des informations par les CMR du régime d'assurance maladie des travailleurs indépendants devraient figurer dans l'arrêté qui fixe les règles auxquelles doivent satisfaire les traitements opérés pour l'exploitation des informations fiscales, conformément au II de l'article 2 du décret du 14 décembre 1999.

En ce qui concerne les informations fiscales communiquées aux organismes de sécurité sociale

— Pour les informations relatives aux bénéficiaires de prestations sociales sous condition de ressources, sans distinguer entre le régime général et le ré gime agricole

Les informations fiscales demandées concernent l'allocataire et, s'il y a lieu, son concubin, conformément à l'article R. 531-10 du code de la Sécurité sociale.

Deux fichiers de restitutions successifs sont constitués pour la communication par la DGI :

— d'informations issues des déclarations d'ensemble des revenus de l'année N -1, plus particulièrement des montants inscrits par les contribua bles aux rubriques énumérées dans les annexes des arrêtés soumis à la CNIL;

— des rectifications apportées à l'imposition primitive par les contribuables ou par les services fiscaux aux mêmes rubriques, en cas d'émission de rôles supplémentaires ou de dégrèvements ;

— du numéro d'ordre du traitement de l'imposition et du numéro du rôle d'émission, afin de permettre aux agents qui utiliseront les informations cor respondantes d'en apprécier le niveau d'actualisation.

— Pour les informations relatives aux personnes relevant du régime général ou du régime agricole de l'assurance vieillesse

Les catégories d'informations enregistrées dans les fichiers de restitutions constitués à cette fin concernent les seuls pensionnés. Il s'agit :

— d'un code « imposé » ou « affranchi » au regard de l'article 1417-1 et III du code général des impôts ;

— d'un code « exonéré » ou « recouvré » au regard de l'article 1657-1 bis du CGI ;

— des rectifications apportées à ces codes en cas d'envoi d'une situation fiscale corrective ;
— du numéro d'ordre du traitement de l'imposition et du numéro du rôle d'émission.

— Pour les informations relatives aux personnes relevant du régime d'assu rance maladie des travailleurs indépendants

La liste précise des catégories d'informations fiscales transmises est fixée par l'arrêté qui régit ces transferts. Elles concernent tant les impositions primitives que les situations fiscales correctives et sont issues :
— des déclarations d'ensemble de revenus, pour les assurés sociaux rele vant du régime de l'article 62 du CGI, du régime de l'article 93-1 ter du CGI, du régime des micro-entreprises ou du régime spécial des bénéfices non commerciaux,
— des liasses fiscales transmises à l'appui des déclarations de résultat, pour les assurés sociaux ne relevant d'aucun de ces régimes fiscaux.

La Commission constate que de très nombreuses informations fiscales susceptibles de figurer sur le formulaire 2042 de la déclaration d'ensemble de revenus ou sur les liasses fiscales pourront être transmises aux organismes de sécurité sociale participant à la procédure « TDF ».

Elle estime cependant, eu égard d'une part à l'extrême détail des rubriques de ces documents et d'autre part à la nécessité de faire coïncider les données transmises avec les catégories de ressources distinguées par le code de la sécurité sociale, que les informations qu'il est prévu de transmettre sont celles qui sont nécessaires pour atteindre les finalités autorisées par la loi. Elles sont donc adéquates et pertinentes et n'appellent pas d'autre observation de la part de la Commission.

En ce qui concerne les modalités de transmission des informations fiscales aux organismes de sécurité sociale

— La constitution des fichiers d'appels

Les transferts d'informations sont effectués sur la base de fichiers d'appels constitués sous le contrôle de l'organisme demandeur. Il a été indiqué à la Commission qu'en l'état actuel des choses, pour des raisons tenant au calendrier des traitements informatiques de la DGI, les fichiers d'appels créés pour le contrôle des droits à prestations sous condition de ressources sont constitués alors que la population des bénéficiaires de l'année N n'est pas encore connue et donc sur la base de la population des bénéficiaires de l'année N -1. Il en résulte que sont mentionnées, dans les fichiers d'appels, des personnes dont les ressources n'auront pas à être contrôlées par l'organisme demandeur et que, dans cette mesure, les informations transmises ne sont pas strictement nécessaires au sens de l'article R.* 152 du LPF.

La Commission souhaite qu'à terme, et au plus tard en 2005, les modalités de constitution des fichiers d'appels soient revues afin que ceux-ci ne comportent plus que des demandes d'informations relatives :

— aux personnes ayant demandé à bénéficier d'une ou plusieurs des prestations précitées pour l'année N et ayant fait parvenir à cette fin une déclaration de ressources ;

— aux personnes indiquées comme vivant maritalement avec un allocataire sur les déclarations transmises pour cette année ;

— aux personnes ayant vocation, au vu de leur situation financière et des réglementation applicables, à bénéficier d'une prolongation des droits pendant quelques mois en l'absence de déclaration déposée dans les délais impartis.

Dans l'immédiat, il a été assuré qu'à l'issue du rapprochement des informations transmises par le CNTDF et des données déclaratives enregistrées dans les fichiers des CAF, les informations fiscales concernant des personnes qui ne sont plus bénéficiaires de prestations soumises à condition de ressources ne sont ni conservées dans les centres informatiques de la CNAF après le traitement des fichiers de restitutions, ni intégrées dans les applications « CRISTAL » des CAF, ni communiquées à ces organismes sur un autre support et que toute mesure utile serait prise à cette fin.

La Commission prend acte de cet engagement dont le respect constitue une condition de validité de la procédure.

En outre, les mêmes garanties devraient être mises en place par les organismes de mutualité sociale agricole.

ta *constitution des fichiers de restitutions*

Selon l'article R.* 152-111 du LPF, les informations demandées ne sont transmises par la DGI qu'en cas de concordance suffisante des éléments d'identification contenus dans la demande avec ceux détenus par l'administration fiscale.

Lorsque les informations fiscales demandées proviennent des fichiers de l'impôt sur le revenu, le processus d'identification des personnes physiques mis en place par la DGI a pour but de retrouver leur identifiant fiscal national — le n° SPI — qui sera utilisé pour retrouver le numéro du foyer fiscal, sur la base duquel les fichiers de taxation de l'administration fiscale sont ultérieurement interrogés. Dans un premier temps, la procédure d'identification s'effectue sur la base du NIR et fait intervenir un « fichier de correspondance NIR/ n° SPI » ; lorsque le NIR transmis dans la demande y est trouvé, ce fichier permet de vérifier l'identité parfaite des NIR et des premiers caractères du nom patronymique. Ce « fichier de correspondance NIR /n° SPI » est géré par le CNTDF et ne sert qu'à la réalisation des transferts de l'article L. 152 du LPF.

Outre les informations détenues par la DGI dans ses propres fichiers, à finalité fiscale, la table de correspondance du CNTDF comporte les NIR transmis par les organismes de sécurité sociale dont ne dispose pas l'administration fiscale et dont les titulaires n'ont pu être identifiés que sur la base d'une procédure plus complexe qui prévoit le rapprochement de l'ensemble des éléments d'état civil et d'adresse enregistrés dans le fichier d'appels et de ceux détenus par la DGI et recourt à un système automatisé d'évaluation du degré de concordance. Le seul objet de la conservation des NIR ainsi attribués est d'éviter le renouvellement chaque année de ces lourds travaux d'identification.

La Commission se félicite qu'ainsi, les rapprochements de fichiers ne s'effectuent jamais sur la seule base du NIR et que la circulation de cet identifiant soit limitée à ce qui est strictement indispensable.

Elle rappelle, par ailleurs, que les procédures de certification de cet identifiant auprès de l'INSEE ont pour objet de garantir leur attribution au bon titulaire et devraient donc être encouragées.

En ce qui concerne l'information des personnes sur les conditions d'exploitation des données fiscales

Le formulaire de déclaration d'impôt sur le revenu pour 2000 informe les contribuables que « les caisses d'allocations familiales, les organismes chargés du paiement des pensions de retraite du régime général, les caisses de Mutualité sociale agricole et les caisses d'assurance maladie des professions indépendantes seront, sur leur demande, destinataires des informations issues du traitement de l'impôt sur le revenu de leurs allocataires, pensionnés ou assurés ».

La déclaration de ressources de la CNAF comporte l'indication suivante : « je prends connaissance que ma caisse vérifiera l'exactitude de cette déclaration auprès de l'administration des impôts ».

La déclaration de ressources de la Mutualité sociale agricole explique : « la MSA peut vérifier l'exactitude des déclarations qui lui sont faites (article L. 583.3 du code de la Sécurité sociale), notamment auprès de l'administration fiscale ».

Le formulaire de déclaration commune des revenus des professions indépendantes utilisé par la CANAM prévient : « les déclarations communes de revenus des professions indépendantes peuvent être transmises, pour contrôle, à l'administration fiscale (article L. 152 du Livre des procédures fiscales) ».

Les courriers adressés chaque début d'année par la CNAVTS pour aider les retraités à compléter leur déclaration fiscale de revenus, précisent : « si vous êtes domiciliés fiscalement en France, la direction générale des impôts nous communique votre situation fiscale. Il est donc inutile de nous adresser votre avis d'impôt sur le revenu, sauf demande expresse de notre part ».

La Commission estime que les formulaires de déclaration de ressources utilisés par les CAF et les caisses de MSA devraient expliquer que des informations issues des déclarations de revenus seront demandées à l'administration fiscale et que les droits à prestations pourront être déterminés en tenant compte de ces dernières informations.

Il conviendrait de même que les formulaires de déclaration commune de revenus utilisés par la CANAM précisent que ces déclarations seront rapprochées des informations relatives à la situation fiscale de l'assuré social qui sont transmises par la direction générale des impôts.

Enfin, la MSA devrait informer ses retraités des transferts mis en place dans des conditions analogues à celles retenues par la CNAVTS.

En ce qui concerne les mesures de sécurité adoptées

Les traitements du CNTDF sont effectués sur une plate-forme dédiée. En outre, des supports informatiques distincts et des fichiers dédiés sont utilisés pour la conservation du fichier de correspondance NIR/n° SPI et la sauvegarde des fichiers d'appels.

Les opérations de mise en exploitation et de maintenance et les opérations courantes d'exploitation des fichiers et traitements mettant en œuvre le NIR sont effectuées par des agents bénéficiant d'une habilitation spéciale. Elles sont organisées et vérifiées dans des conditions conformes aux engagements constatés par la délibération de la CNIL n° 99-060 du 9 décembre 1999.

Les projets d'arrêtés soumis à la CNIL prévoient que les fichiers d'appels et de restitutions seront systématiquement chiffrés pendant leur transmission, au plus tard à compter du 31 décembre 2005.

La Commission exprime le souhait que ce dispositif soit opérationnel avant la fin de l'année 2003 et rappelle que le chiffrement devra être mis en place pour l'ensemble des transmissions de fichiers, non seulement entre les centres informatiques des organismes de Sécurité sociale et le CNTDF mais aussi entre ces structures nationales et les organismes ou services locaux amenés à traiter les fichiers d'appels ou de restitutions, que ces transferts soient effectués par réseau télématique ou sur support magnétique.

La Commission considère, en outre, qu'il serait souhaitable qu'un audit externe de sécurité soit réalisé à périodicité régulière.

Au bénéfice de ces observations, la Commission émet un avis favorable sur l'ensemble du dispositif qui lui est présenté.

La Commission demande, par ailleurs, au comité de gestion de la procédure « TDF » de lui faire parvenir annuellement un bilan portant sur les conditions d'application de la procédure de transfert de données fiscales.

III. LES LISTES NOIRES

Une « liste noire » est, dans le vocabulaire courant, une liste de personnes jugées indésirables ou dont certains comportements appellent à la vigilance. La loi du 6 janvier 1978 garantit que de telles listes « d'indésirables » ne puissent constituer des « casiers judiciaires parallèles » non contrôlés et reconnaît aux personnes concernées, comme à toute personne susceptible d'être fichée, des droits particuliers : droit à l'information préalable, droit d'accès, droit d'opposition pour raison légitime, droit à l'oubli.

L'exercice de ces droits suffit-il à prévenir toute dérive ? Rien n'est moins sûr. En tout cas la tendance est fermement dessinée : les professionnels font valoir la nécessité de se protéger contre la fraude ou le risque d'impayé pour mettre en commun les informations dont ils disposent sur certains clients dont le comportement ou l'absence de loyauté à leur égard leur a causé préjudice.

Quelquefois de tels fichiers sont destinés à protéger les personnes contre elles-mêmes, ainsi du Fichier des incidents de remboursement de crédit aux particuliers (FICP) mis en place par la Banque de France, pour prévenir les cas de surendettement en recensant l'ensemble des impayés de crédit. Parfois ces fichiers sont destinés à protéger les personnes contre les comportements de tiers, c'est le cas du Fichier central des chèques (FCC) qui recense notamment les références des chéquiers volés et des cartes bancaires en opposition afin de prévenir tout nouvel usage de ces moyens de paiement irréguliers.

Mais au-delà de quelques lois particulières qui sont intervenues afin de mieux encadrer le fonctionnement de tels fichiers, des groupements professionnels ou des sociétés privées sont de plus en plus nombreux à offrir des services de « repérage » ou de recensement des clients dits « à risques ».

L'inscription d'une personne dans un tel fichier a un effet stigmatisant qui peut, quelquefois, revêtir un caractère disproportionné par rapport aux faits reprochés. En outre, de tels fichiers sont très largement dérogatoires aux principes généraux de la protection des données personnelles puisque, loin de demeurer confidentielles, les informations en cause sont alors partagées, c'est-à-dire portées à la connaissance des acteurs professionnels concernés. Enfin, par leur fonctionnement même, ces « listes noires » paraissent contraires à la philosophie du « droit à l'oubli » puisqu'elles vont attacher à une personne un de ses comportements passés afin d'alerter l'ensemble d'un secteur professionnel susceptible de contracter avec la personne concernée.

En matière de crédit à la consommation, le développement des « fichiers communs d'incidents » est pour partie la conséquence d'une « philosophie française » qui tend à faire prévaloir les fichiers dits « négatifs », recensant les seuls incidents de paiement, sur les fichiers « positifs » recensant, eux, la totalité des encours. Aux États-Unis et en Grande-Bretagne, tout particulièrement, l'approche est différente et repose sur les fichiers « positifs ». Une meilleure connaissance du client permettrait l'octroi d'un crédit plus adapté, mieux maîtrisé et plus important que la seule utilisation d'un fichier d'incidents de paiement. En outre, un fichier d'encours ne revêtirait pas, à la différence d'un fichier « négatif », l'aspect péjoratif de liste d'infamie rendant le fichage psychologiquement difficile à vivre. Tels sont les arguments de nombreux professionnels de crédit à l'étranger qui souhaiteraient introduire en France leur savoir faire en matière de centrale positive.

Ces arguments ne sont pas sans force mais n'ont jusqu'à présent pas pleinement convaincu.

En terme de protection de la vie privée, un fichier « négatif » comporte moins de données et concerne moins de personnes qu'un fichier « positif » qui se prête, par son exhaustivité et la connaissance qu'il apporte non seulement sur le volume des crédits souscrits mais aussi sur l'objet des crédits, à des détournements de finalité et notamment, à un ciblage des personnes en vue de les démarcher commercialement. La Commission s'est toujours interrogée sur la légitimité qu'il y aurait pour un organisme prêteur à accéder à des données personnelles portant sur les crédits contractés avec des tiers dès lors que l'emprunteur remplit normalement ses obligations contractuelles et n'a été l'objet d'aucun incident de paiement.

En terme d'efficacité pour les professionnels de crédit, il est loin d'être acquis que le taux d'impayés serait moindre dans l'hypothèse d'une mise en œuvre d'un fichier « positif ». Ainsi, le taux d'impayés au Royaume-Uni qui dispose pourtant de deux centrales « positives » est de même niveau qu'en France.

En outre, un fichier « positif » peut générer d'autres effets pervers. Ainsi, certains établissements spécialisés peuvent racheter les créances de leurs meilleurs clients ; des établissements soucieux de ne pas voir partir leurs « bons clients » peuvent faire de fausses déclarations avec tous les risques que cela comporte pour les personnes concernées ; le consommateur, fortement sollicité, peut être poussé aux limites de ses possibilités financières.

Enfin, l'existence d'un fichier « positif » n'a jamais mis un terme à la prolifération de « listes noires ». Les uns et les autres coexistent et certaines sociétés, notamment anglo-saxonnes, offrent à la fois un service de centrales positives et un service de fichiers d'incidents.

Aussi, si le débat sur les avantages et les inconvénients comparés entre fichiers « positifs » et fichiers « négatifs » est loin d'être clos et mérite d'être poursuivi en liaison avec les professionnels concernés et les associations de consommateurs, la question des « listes noires » et des fichiers « d'incidents » demeure.

Ces derniers appellent assurément à une grande vigilance et la Commission a noté que la directive européenne du 24 octobre 1995 cite parmi les traitements « susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées » et appelés, à ce titre, à pouvoir faire l'objet d'un examen préalable par l'autorité de contrôle avant toute mise en œuvre, les traitements ayant pour finalité « d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ». Car telle est bien la finalité de cette « mutualisation » d'informations destinées à prévenir la fraude ou l'impayé : non pas conduire systématiquement à dénier un droit ou refuser un service à une personne en particulier mais permettre à des professionnels de connaître « le profil » de certaines personnes et de décider, en toute connaissance de cause, de contracter, le cas échéant, en en fixant des conditions particulières, ou de ne pas contracter.

La Commission a été saisie dans le courant de l'année 2001 de plusieurs déclarations de traitements ayant pour objet d'apprécier le risque éventuel présenté par certaines personnes : risque d'insolvabilité des demandeurs de crédit, antécédents des incidents de paiements pour les professionnels de l'immobilier, de l'assurance ou de la téléphonie. Elle a examiné à plusieurs reprises en séance plénière ces traitements afin de veiller à la mise en œuvre de garanties minimales dont il lui appartiendra ensuite de contrôler l'effectivité. Cependant, en l'état de la loi du 6 janvier 1978 qui, dans l'attente de la transposition de la directive européenne, ne soumet pas les fichiers informatisés du secteur privé à un examen préalable mais à un régime de simple déclaration contre délivrance d'un récépissé, cet encadrement juridique n'est pas toujours effectif. Aussi, la CNIL a-t-elle alerté à ce sujet les pouvoirs publics. Dans l'attente d'une évolution de la loi dans ce domaine, et compte tenu de leur sensibilité, de tels traitements font systématiquement l'objet de vérifications sur place.

A. La déclaration d'un outil commun de lutte contre la fraude dans le secteur du crédit

La société Experian qui compte parmi les leaders mondiaux de la fourniture, du traitement et de l'analyse de l'information a déposé auprès de la Commission plusieurs déclarations de traitements. Ce groupe international est implanté dans seize pays et réunit plus de 10 500 salariés.

En France, Experian, avec 1 500 collaborateurs, déploie ses offres sur quatre marchés : la banque, la finance et l'assurance, la distribution et la grande consommation, les télécommunications et services, enfin les administrations et

services publics. Experian est aujourd'hui leader mondial du géomarketing et a développé une base de données découpant le territoire national en 300 000 pâtés de maisons et 22 millions de foyers consommateurs qualifiés et localisés dont les données sont croisées, valorisées et transformées en informations à partir de données cartographiques/socio-démographiques et économiques, de consommation et de comportement.

Dans le secteur du crédit, Experian a développé dans plusieurs pays des services de centrales d'informations, parmi lesquelles figurent les fichiers « positifs », qui recensent non pas seulement les incidents de paiement en matière de crédit mais tous les encours de crédit. C'est ainsi qu'aux USA, Experian fut la première société à proposer un système d'informations automatisé relatif aux crédits souscrits par les consommateurs et traite aujourd'hui plus d'un million de requêtes de crédit chaque jour. Ainsi, File One, la base de donnée d'Experian, comporte des informations se rapportant à plus de 205 millions de consommateurs américains et comprend non seulement une information globale et détaillée sur les crédits fournis par les principaux établissements de crédit, mais aussi les jugements et faillites, des données relatives aux recouvrements et à l'emploi et des informations sur les recherches précédemment effectuées.

En Europe, Experian démarra par la Grande-Bretagne en 1980 par la constitution d'une centrale positive en matière de crédit traitant 70 % des requêtes dans ce domaine, soit plus d'un million de requêtes chaque semaine.

Experian souhaite constituer en France une base mutualisée de chacun des fichiers de lutte contre la fraude mis en œuvre dans les établissements de crédit qui sont ses adhérents, afin de permettre à ceux-ci de se prémunir contre les tentatives de fraude et/ou de récidive. L'objectif annoncé par cette société est de sécuriser l'octroi de crédit et de permettre son développement. Elle fait notamment valoir que le marché français du crédit à la consommation est moins important que dans les autres pays européens et a *fortiori* aux États-Unis. Les crédits de trésorerie et les crédits à la consommation ne représenteraient en effet que 8 % du revenu des ménages français contre 16 % en Allemagne et 28 % aux USA.

Experian prévoit que les adhérents doivent fournir les données issues de leur propre fichier « fraude » à la centrale afin de recevoir, en contrepartie, les informations figurant dans la base en provenance d'autres établissements de crédit. Certains établissements clients d'Experian pourront adhérer au système d'information tout en ne l'alimentant pas. Dans ce cas, ils auront alors seulement connaissance de l'existence d'un dossier fraude sous la forme « oui/non ». Dans les deux cas, il ne peut s'agir que d'établissements autorisés à effectuer des opérations de crédit, telles qu'elles sont définies dans la « loi bancaire » du 24 janvier 1984, et la décision finale d'octroi du crédit reste, évidemment, du ressort exclusif de l'établissement bancaire ou financier. Ainsi, Experian ne donne aux adhérents que le résultat de leurs requêtes, à charge pour ces derniers soit de donner rapidement un accord sur l'octroi d'un crédit soit de demander des garanties supplémentaires, soit, évidemment, de refuser d'accorder le crédit.

Experian fait valoir que les adhérents devront garantir la confidentialité et la sécurité des informations qui leur seront transmises ainsi qu'une utilisation des informations conforme à la finalité déclarée du traitement. À cette fin, Experian fait signer à chaque client une « charte Experian » dont le non respect engage la responsabilité de l'adhérent. Chaque adhérent sera responsable de l'emploi qu'il fera des résultats et à ce titre s'engage à ne pas interroger la base à d'autres fins que celles prévues. Chaque adhérent devra, pour se connecter à la base centralisée, utiliser obligatoirement les codes identifiants qu'Experian lui aura remis préalablement et s'assurer que seules les personnes habilitées à interroger la base auront accès aux données.

Les engagements pris par Experian ne sont pas de nature à apaiser les craintes de la Commission à l'égard d'une telle initiative.

Un fichier commun de lutte contre la fraude est par nature beaucoup plus sensible qu'un fichier commun d'impayés car si l'impayé est un fait objectif et de nature civile, la fraude est évidemment beaucoup plus subjective et de nature pénale. En outre, l'article 30 de la loi du 6 janvier 1978 réserve le traitement d'informations nominatives concernant des infractions aux juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la CNIL, aux personnes morales gérant un service public.

La Commission a considéré que cette disposition ne fait nullement obstacle à ce qu'un organisme dans le cadre de sa gestion interne puisse, sous certaines garanties contrôlées par la CNIL, conserver trace d'un agissement lui ayant porté préjudice pour se prémunir de tout éventuel renouvellement à son égard *[cf.* 15e rapport d'activité 1994, p. 134). Par contre, paraissent entrer dans les prévisions de l'article 30 de la loi, la centralisation de toutes les fraudes ou tentatives de fraude — classées en différentes catégories selon le degré de gravité que les établissements leur confèrent — et surtout la diffusion de telles informations — quelle qu'en soit la forme, fût-ce sous celle réduite attestant l'existence ou l'absence d'une fraude précédemment signalée par autrui — à des tiers n'ayant subi aucun préjudice direct.

Ainsi, si la Commission est parfaitement consciente de la légitimité pour les professionnels du crédit de souhaiter s'organiser à cet égard, comme elle l'a déjà précisé dans son rapport d'ensemble sur « La prévention de la fraude et des impayés dans le crédit à la consommation » *[cf.* 21e rapport d'activité 2000, p. 168), elle observe que l'article 226-19 du code pénal punit de cinq ans d'emprisonnement et de 2 000 000 F d'amende le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des informations nominatives concernant des infractions, des condamnations ou des mesures de sûreté. La mise en oeuvre d'un traitement regroupant notamment les délits de faux ou d'escroquerie que les établissements de crédit imputeraient à des personnes nominativement désignées et la diffusion de telles « listes noires » à l'ensemble des professionnels pourraient tomber sous la prévision de ce texte.

De surcroît, le secteur du crédit étant régi par le secret bancaire, la centralisation et l'accessibilité à des tiers d'informations nominatives couvertes par le secret professionnel soulèvent une autre difficulté juridique d'importance. En effet, si Experian a fait valoir qu'il reviendrait à chaque adhérent d'obtenir préalablement à

l'enregistrement de tout dossier dans la base centrale la levée du secret bancaire par la personne concernée dans ledit dossier, c'est-à-dire le recueil de son autorisation à ce que le secret bancaire soit levé, la Commission nourrit des doutes sur la validité juridique de telles pratiques et sur leur compatibilité avec des dispositions d'ordre public.

Cependant, la procédure prévue par la loi du 6 janvier 1978 pour les fichiers privés étant celle d'une simple déclaration contre délivrance d'un récépissé, la Commission ne dispose pas de la faculté d'empêcher la mise en œuvre de ce type de fichiers. C'est la raison pour laquelle elle a souhaité attirer l'attention du ministère de la Justice par un courrier du 13 juillet 2001 sur les lacunes de la loi en ce domaine.

En effet, si le développement et sans doute le changement de nature de la fraude au crédit rendent légitimé le souhait des professionnels de s'organiser au mieux pour se prémunir, seule une intervention législative spécifique parait de nature à concilier les obligations des professionnels et les droits des personnes concernées, en imposant des règles communes notamment sur les garanties et conditions minimales d'inscription dans de tels fichiers et, le cas échéant, la durée de conservation des informations.

À défaut d'une telle disposition législative, il n'est pas à exclure que les professionnels pourraient mettre à profit les délais de mise en œuvre de la future loi modifiant la loi du 6 janvier 1978 — et qui devrait, sur ce point, renforcer considérablement les moyens de la Commission sur les fichiers de ce type — pour multiplier rapidement les initiatives de cette nature générant ainsi une prolifération de « listes noires » sans réelles garanties pour les personnes concernées.

À ce jour, cependant, la société Experian n'a pas fait savoir à la Commission si, à la suite de ses observations générales, elle entendait ou non mettre en œuvre le projet déclaré à la CNIL.

B. La mutualisation des incohérences détectées dans les demandes de crédit

La même société Experian a déposé auprès de la Commission une autre déclaration de traitement consistant à recueillir dans une base centrale, les informations déclarées par un demandeur de crédit afin, le cas échéant, de pouvoir les comparer avec les informations précédemment déclarées auprès d'un autre établissement (identité, adresse, revenus, endettement déclaré et toutes données transmises à l'occasion d'une demande de crédit telles l'ancienneté dans l'établissement bancaire ou dans l'emploi). Il ne s'agit pas alors de recenser dans un même fichier les comportements jugés frauduleux mais de repérer par comparaison entre des éléments objectifs communiqués par le demandeur à un établissement de crédit certaines divergences ou anomalies, lesquelles peuvent appeler à une vigilance particulière, sinon nourrir une suspicion de fausse déclaration.

Le contrôle de cohérence s'effectue par la comparaison des éléments fournis dans la demande de crédit avec des informations publiques, issues par exemple d'annuaires publics, mais également avec les informations recueillies précédemment pour le même client, à l'occasion d'une demande de crédit antérieure. Le traitement produit alors des codes d'alertes en cas de non-concordance du rapprochement des diverses données stockées.

La loi du 6 janvier 1978 s'applique bien évidemment à un tel traitement, puisqu'il est le fruit d'un rapprochement de traitements épars mis en œuvre par chaque établissement de crédit qui se trouvent au moins pour partie regroupés entre les mains d'un même opérateur, et va permettre de produire des informations nouvelles et jusqu'alors inconnues de chacune des établissements de crédit : le défaut de concordance entre les informations dites « de base ».

Experian fait valoir qu'une telle évolution serait justifiée par un phénomène connu sous son nom anglais de « *credit shopping »* qui décrit le comportement d'un consommateur se livrant soit, aux fins d'une mise en concurrence de l'offre de crédit, ou parfois afin « d'améliorer » son profil pour augmenter sa capacité d'emprunt, au démarchage systématique d'un grand nombre d'établissements de crédit. C'est cette seconde pratique, préjudiciable tant à l'établissement de crédit qui ne dispose pas d'un outil complet d'évaluation du risque qu'au consommateur, lequel compromettrait sa situation par l'obtention d'un crédit trop élevé pour lui et s'exposerait ainsi à un risque de surendettement, qui justifierait la mise en oeuvre d'une telle mutualisation.

Une telle mutualisation ne remet pas en cause ce que l'on peut qualifier de principe de « neutralité » des services offerts puisqu'elle n'a pas pour objet de permettre aux adhérents d'enrichir leur propre fichier interne mais de leur apporter une information destinée à éclairer la décision à prendre.

L'information préalable du client sur le système incombe à l'adhérent qui doit recueillir le consentement écrit du client. Une formule type est préconisée par Experian : « *Les informations contenues dans votre demande de crédit seront susceptibles d'être transmises à un fichier centralisé géré par la société EXPERIAN et accessible à l'ensemble des établissements bancaires et financiers adhérents dudit fichier centralisé ».*

Lors de l'instruction de ce dossier, la Commission a particulièrement insisté sur l'information des personnes afin qu'il puisse être considéré que leur consentement éclairé est bien recueilli. La Commission a, en particulier, jugé nécessaire qu'Experian apparaisse clairement comme destinataire des informations dans la mesure où cette dernière est la seule à disposer de l'ensemble des informations et que le droit d'accès des personnes concernées doit également porter sur le résultat du contrôle de cohérence.

Là encore, ce dossier de déclaration étant formellement complet, la CNIL n'a pu que délivrer le récépissé de la déclaration. Elle a toutefois rappelé que la délivrance de ce récépissé n'exonère en aucun cas des éventuelles responsabilités pénales et civiles et a attiré l'attention du déclarant sur plusieurs points sensibles.

La mutualisation des fichiers traitant de données couvertes par le secret bancaire n'est en effet admissible qu'à certaines conditions.

Ainsi, au regard des articles L. 511-33 et L. 511-34 du code monétaire et financier relatifs au secret bancaire, la mutualisation des données relevant du secret bancaire ne semble envisageable qu'à la condition d'une autorisation explicite des clients intéressés à voir levée, au profit de la société Experian, l'obligation de secret professionnel auquel sont tenus les établissements de crédit. Une simple mention d'information sur ce point pourrait ne pas être conforme aux textes légaux.

La Commission a considéré, en outre, que la suspension de l'accès d'un des adhérents à la Centrale en raison du caractère « insatisfaisant » de la qualité des données communiquées devrait entraîner le retrait — au moins temporaire — de toutes informations enregistrées dans la base à son initiative.

Enfin, la Commission a cru devoir préciser qu'en l'état de la loi n° 89-1010 du 31 décembre 1989 *[JO* 2/1/90) relative au FICP, la mise en place d'une centrale positive des encours de crédit serait contraire aux orientations arrêtées par le législateur.

C. La prévention des impayés dans les services de téléphonie

Dès 1996, les opérateurs de téléphonie mobile (SFR, Orange et Bouygues Télécom depuis l'année 2000) et certaines sociétés de commercialisation de services (SCS) se sont regroupées au sein d'un GIE dans le seul but de pouvoir mettre en œuvre un traitement (« Préventel ») de prévention des impayés par la centralisation d'informations relatives à des impayés et des anomalies constatés auprès de leurs abonnés au service de téléphonie mobile, survenant lors de la souscription ou de l'exécution des contrats d'abonnement tant particuliers qu'entreprises.

Ce traitement a fait l'objet en novembre 1996 d'une déclaration à la Commission, conformément à l'article 16 de la loi du 6 janvier 1978.

La finalité d'un tel fichier pour les opérateurs est double. Il s'agit tout d'abord de fournir un élément d'appréciation des demandes de souscription de contrats d'abonnement. À cet égard, le recensement dans le fichier ne constitue pas automatiquement un obstacle à la souscription d'un contrat mais avertit l'opérateur sur les risques possibles liés au recouvrement des futures créances. Il lui appartient alors de définir la stratégie à adopter : demande d'un dépôt de garantie, refus de contracter, etc. Par ailleurs, le fichier permet la mise en œuvre d'un dispositif de vérification des informations fournies lors d'une demande d'abonnement afin de prévenir les souscriptions de contrats irrégulières et successives auprès de plusieurs membres.

Les règles de gestion du fichier Préventel reprennent, classiquement, celles en vigueur concernant la tenue de « listes noires », à savoir :

— l'inscription des seules créances uniquement relatives à un impayé d'un montant supérieur à un seuil significatif de 500 F ;

— la suppression de l'inscription dès règlement par le débiteur et en tout état de cause après trois années ;
— la présence de l'information relative au GIE Preventel dans le contrat et lors de l'opération d'inscription avec l'indication des coordonnées postales du GIE ;
— l'indication de la date et du lieu de naissance afin de prévenir tout risque d'homo nymie.

Compte tenu des nombreuses plaintes émanant de particuliers relatives à l'existence ou à la tenue du fichier Preventel, la Commission, par une délibération du 30 novembre 2000, a décidé d'une mission de vérification sur place tant auprès du GIE, que de ses membres (au total, dix contrôles ont été effectués). À l'issue de ces missions, la Commission a été amenée à rappeler un certain nombre de principes.

En premier lieu, seul un impayé supérieur ou égal au montant défini par le GIE doit conduire à une inscription.

En deuxième lieu, il incombe au GIE et à ses membres de s'assurer de la réalité de la dette. Ainsi, en cas de contestation, l'inscription au fichier Preventel ne devrait avoir lieu qu'après intervention afin de procéder à un examen spécifique et contradictoire de la réalité de la dette.

Enfin, la Commission a préconisé au GIE une refonte de son code « anomalie » afin de rendre ce dernier compatible avec les exigences de l'article 30 de la loi du 6 janvier 1978. C'est ainsi que ce code concerne tout à la fois les entreprises qui n'existent pas ou qui n'existent plus (en liquidation judiciaire ou radiées), les retours de courriers « NPAI » (n'habite plus à l'adresse indiquée), les comptes bancaires inexistants et les documents présentant des ratures, sur charges... Dès lors, les éléments qui pouvaient tomber sous le coup de l'article 30 qui prohibe le recensement d'infractions sont englobés dans un code ne permettant pas de faire ressortir des informations d'une telle nature.

Avec l'ouverture à la concurrence depuis le 1er janvier 1998 du secteur des télécommunications fixes et la fusion des différents marchés de la téléphonie, le GIE Preventel s'est ouvert à l'ensemble des opérateurs de téléphonie. Ainsi, depuis mars 2002, le fichier Preventel peut être considéré comme le fichier recensant les incidents de paiement concernant l'ensemble des opérateurs de télécommunications, à l'exception notable de France Télécom.

L'ouverture du GIE aux opérateurs filaires avait semblé justifiée à la CNIL compte tenu de l'évolution du marché de la téléphonie qui tend à supprimer la distinction originelle entre téléphonie fixe et téléphonie mobile. La Commission a, en revanche, exprimé de vives réserves aux autres modifications envisagées par le GIE.

En effet, l'évolution du fichier Preventel ne s'est pas limitée à une ouverture à de nouveaux membres mais a conduit, de façon plus générale, à l'extension des conditions d'inscription.

Ainsi, le seuil de l'impayé conduisant à une inscription a été abaissé de 500 francs (environ 70 euros) à 60 euros tandis que |a-durée de conservation des informations relatives aux personnes ayant eu au moins trois notifications distinctes d'impayés a été portée de 3 à 5 ans.

Sur ces points, la Commission a fait savoir au GIE que ces mesures paraissaient excessives au regard du principe de proportionnalité auquel doit obéir la mise en oeuvre d'un traitement de prévention d'impayés dans le domaine de la téléphonie.

La Commission considère tout particulièrement que, s'agissant des clients contestant le montant ou le fondement juridique de la somme dont le paiement leur est réclamé, c'est à l'opérateur d'établir le bien fondé de sa demande de paiement, par une instruction contradictoire de la contestation, conduite dans un délai raisonnable, de façon non automatisée, et assortie surtout de la suspension du processus d'inscription dans le fichier.

Par ailleurs, la Commission a appelé l'attention du GIE sur le fait que la référence à une inscription éventuelle dans le fichier ne devrait pas être utilisée comme une menace pendant la phase de contact avec le débiteur.

La Commission a enfin indiqué au GIE que les fréquents dysfonctionnements affectant la gestion du fichier Preventel provoquent un nombre croissant de plaintes adressées à la CNIL portant le plus souvent sur ces différents points.

C'est pourquoi la Commission a enjoint Preventel de respecter avec soin et en permanence l'intégralité des dispositions de la loi du 6 janvier 1978 et les conditions de mise en œuvre du dispositif, considérant l'afflux d'inscriptions nouvelles et l'augmentation corrélative des plaintes que risquent de générer les modifications apportées au fichier. La Commission y sera pour sa part très attentive.

D. La mutualisation multisectorielle d'incidents de paiement de particuliers

Une société du sud de la France, gestionnaire d'une base de renseignements commerciaux déclarée à la CNIL en 1994 destinée aux cabinets de recouvrement de créances avait, par la suite, mis en place un dispositif dénommé « accélérateur de paiement » consistant à produire automatiquement des lettres à des fins de recouvrement de créances, les courriers étant à l'entête des cabinets de recouvrement abonnés.

Cette société a déposé à la CNIL, fin 2000, une déclaration relative à un nouveau traitement dont l'objectif est de centraliser les incidents de paiements d'entreprises ou de particuliers en matière de logement, de téléphonie et d'assurances pour permettre aux professionnels de chacun de ces secteurs de consulter l'ensemble des impayés enregistrés dans leur secteur d'activité qu'ils soient le fait d'une personne physique ou d'une personne morale.

La Commission, préoccupée par l'ouverture de la consultation du fichier d'incidents sur les créances civiles aux professionnels de l'immobilier, de la téléphonie et des assurances, a examiné en séance plénière à deux reprises ce traitement, les 8 février et 3 avril 2001.

En effet, le traitement dénommé « fichier national des incidents de paiements » est un parfait exemple de la difficulté à trouver le juste arbitrage entre les exigences des professionnels et les droits des consommateurs dans la mesure où, non

seulement il recense les impayés, mais les centralise dans trois secteurs clés d'activités, le logement, la téléphonie et les assurances, qui touchent de très près à la vie quotidienne des personnes.

Le déclarant a précisé que son fichier correspondrait à une demande de diverses professions et qu'il présentait une garantie « de qualité » en termes de crédibilité des informations et du respect des règles que n'offraient pas les professionnels de tel secteur concerné. Il indiquait notamment que son fichier permettrait d'assainir les pratiques actuellement en vigueur dans plusieurs secteurs (le bâtiment, l'immobilier...) d'échanges informels d'informations sur les débiteurs.

La Commission, tenue par les dispositions de l'article 16 de la loi du 6 janvier 1978, a délivré le récépissé tout en attirant l'attention du responsable sur les problèmes soulevés par ce traitement, tant au regard de la loi informatique et liberté, que de l'utilisation de la dénomination « fichier national » qui induit en erreur les personnes sur la portée du traitement. C'est ainsi que, s'agissant des mentions d'information, la Commission a relevé que la formulation retenue par le déclarant donnait à penser que l'inscription au fichier commun serait recommandée par la loi informatique et libertés ! Bien sûr, il n'en est rien. Aussi, la CNIL a-t-elle proposé d'adopter la formulation suivante : « En cas de non règlement dans un délai de huit jours, vous serez inscrit dans le FNIP, accessible aux professionnels du secteur concerné par votre créance. Conformément à l'article 26 de la loi informatique et libertés du 6 janvier 1978, vous bénéficiez d'un droit d'opposition, pour des motifs légitimes, à figurer dans ce traitement. En cas de contestation, il est impératif de nous adresser les pièces justificatives et de régler la partie non contestée directement chez le créancier. Vous bénéficiez, également en vertu de cette loi, d'un droit d'accès et de rectification aux données enregistrées vous concernant en nous écrivant à l'adresse ci-dessous ». Cette formulation a été retenue par le déclarant.

La Commission a considéré que cette société ne devait à aucun titre faire référence à un label, agrément ou autorisation de la CNIL dans la mesure où la mise en œuvre d'un tel fichier ne relève que de la procédure de déclaration contre délivrance d'un récépissé qui ne s'apparente en rien à un aval de la Commission. Elle a demandé, afin que les clients abonnés au service soient conscients de leur responsabilité, que les conditions générales de vente précisent que l'utilisateur ne peut exploiter l'information recueillie que pour le secteur d'activité considéré sous peine d'application des sanctions pénales prévues en cas de détournement de finalité des informations.

Par ailleurs, la Commission a rappelé son souci que soit préservée l'étanchéité des informations par secteur d'activité, c'est-à-dire qu'un professionnel de l'immobilier, par exemple, ne puisse avoir accès qu'aux impayés déclarés par d'autres professionnels de l'immobilier et non à ceux déclarés par les professionnels de la téléphonie.

La Commission a, en outre, rappelé que ne doivent faire l'objet d'une inscription dans un fichier rendu accessible aux professionnels que les incidents caractérisés de paiement et en application de l'article 29 de la loi, le responsable du traitement devant s'engager à prendre toutes précautions utiles afin de préserver la

sécurité des informations. Les tribunaux ont déjà fait application des sanctions pénales prévues en cas de non respect de ces dispositions, pour défaut d'identification certaine des personnes concernées *[cf.* 16e rapport d'activité 1995, p. 35).

Sur la durée de conservation, la Commission a, compte tenu du risque présenté par la centralisation des incidents, exigeant des garanties supplémentaires par rapport à un fichier sectoriel, maintenu sa préconisation d'une durée de conservation d'informations limitée à trois ans. Bien évidemment, toutes les informations doivent être effacées aussitôt la dette réglée et sans attendre l'expiration de ce délai de trois ans.

Sur ce point, les conditions générales d'utilisation du service précisent que l'abonné devra obligatoirement déclarer toute dette réglée. En cas d'omission, sa responsabilité sera engagée et des dommages intérêts pourront lui être réclamés, même en cas de rupture de l'abonnement. Il y a cependant fort à craindre qu'un abonné qui résilie son contrat ne mette plus à jour la base de données. Dans cette hypothèse, la donnée relative à l'incident régularisé perdurerait dans le fichier pour la durée maximale de conservation. Dès lors, la Commission préconise qu'en cas de résiliation de son contrat par l'abonné, l'ensemble des impayés qu'il avait pu introduire dans la base soit radié.

De plus, la Commission a souhaité rappelé l'attention de la chancellerie et du ministère de l'Économie, des Finances et de l'Industrie sur la multiplication des initiatives privées de recensement des incidents de paiement relatifs à des particuliers qui lui paraît devoir conduire à une intervention législative spécifique sur le sujet.

E. De quelques enseignements...

Au regard d'une tendance qui s'est dessinée il y plus de dix ans et qui avait d'ailleurs conduit la Commission à saisir le Premier ministre de cette question, il convient d'observer que les fichiers désormais mis en oeuvre ne sont plus spécifiques à un secteur d'activité déterminé mais concerne des créances de toute nature relatives aux actes de la vie quotidienne des personnes. Une telle centralisation qui s'apparente à la constitution de véritables fichiers « de mauvais payeurs » très largement consultables est fort stigmatisante pour les personnes concernées et de nature à accroître les risques d'atteinte à leurs droits et libertés. C'est la raison pour laquelle la directive européenne du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données autorise les États membres à subordonner leur mise en oeuvre à un examen préalable de l'autorité de contrôle.

Dans l'attente de la transposition de ce texte dans le droit national, force est de constater que la Commission ne dispose pas, sur le fondement de la loi du 6 janvier 1978, du droit de s'opposer à la mise en œuvre de tels fichiers ni de celui de subordonner leur existence à certaines conditions de fonctionnement, la procédure applicable aux fichiers privés étant celle d'une simple déclaration à la CNIL contre délivrance d'un récépissé. Les pouvoirs de vérification sur place conférés à la Commission par l'article 21 de la loi ne permettent pas davantage à la Commission de prescrire à l'égard de fichiers de cette nature d'autres obligations que celles qui ont été souscrites lors de la déclaration. En particulier, la CNIL ne dispose pas, à l'heure

actuelle, d'un pouvoir d'injonction et ne peut agir que par la concertation et la persuasion.

C'est la raison pour laquelle la Commission s'interroge sur le point de savoir s'il ne conviendrait pas que des garanties minimales de fonctionnement de tels fichiers soient fixées sans tarder par une disposition législative spécifique qui pourrait, le cas échéant, prévoir que ces fichiers ne peuvent être mis en œuvre qu'après autorisation préalable par la CNIL, comme cela a été le cas, ces dernières années, pour les fichiers de recherche médicale ou encore la communication à des tiers d'informations statistiques relatives à l'évaluation des pratiques ou des activités de soins.

Le législateur a déjà réservé à certains opérateurs strictement définis la possibilité de tenir des fichiers nationaux « d'incidents », qu'il s'agisse du fichier national des incidents de remboursement des crédits aux particuliers (FICP) institué par la loi relative au surendettement des ménages du 31 octobre 1989 ou encore du fichier de sécurité des chèques et des cartes de paiement institué par la loi du 30 décembre 1991.

Les tendances du marché que la Commission peut observer dans le cadre de ses missions dictent l'urgence à agir. Ainsi, la CNIL a-t-elle été saisie par la succursale d'une société espagnole, spécialée depuis vingt ans dans le recouvrement de créances, et qui est installée en France depuis octobre 2000. Cette société se propose de constituer un fichier national de tous les incidents de paiement, dans tous les secteurs professionnels, y compris les simples retards, et consultable par toute personne abonnée à ce service.

Par délibération n°01-063 du 13 novembre 2001, la CNIL a décidé de procéder à une mission de vérification sur place auprès du responsable du « fichier national des incidents de paiement » afin de vérifier le respect des préconisations de la CNIL

Enfin, afin de mieux sensibiliser les acteurs professionnels sur les obligations qui leur incombent en vertu de la loi et les consommateurs sur les tendances du marché qu'elle voit à l'œuvre, la Commission a décidé, à la fin de l'année 2001, la création d'un groupe de travail sur les traitements de personnes à risque. Ce groupe de travail a procédé à de nombreuses consultations et tiendra évidemment à la disposition des pouvoirs publics les lignes conclusives qu'il aura dégagées sur ce sujet éminemment sensible.

IV. UN SIECLE DE BIOMETRIE

La biométrie est généralement citée au titre des nouvelles technologies appelées à connaître un fort développement dans les prochaines années. On peut définir les systèmes biométriques comme étant des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques

(empreintes digitales, iris de l'œil, contour de la main, etc.), de traces (ADN, sang, odeurs), ou d'éléments comportementaux (signature, démarche).

La Commission a précédemment consacré de nombreux développements à certaines techniques biométriques, qu'il s'agisse de l'identification par l'ADN (cf. 20e rapport pour 1999, p. 29 *sqq)* ou de l'empreinte digitale *(cf.* 21e rapport d'activité pour 2000, p. 101). Mais les éléments biométriques se diversifient, le marché de la biométrie s'étend et certaines techniques de reconnaissance ou d'identification biométrique soulèvent des problèmes éthiques nouveaux, tels que, par exemple, la reconnaissance des visages. Ces constatations ont conduit la Commission à entreprendre une étude d'ensemble de ces technologies qui sont de plus en plus fréquemment employées en raison notamment d'une baisse considérable de leur coût.

A. Quelques observations techniques

1 — LES CARACTÉRISTIQUES COMMUNES DES ÉLÉMENTS BIOMÉTRIQUES

L'universalité : l'élément biométrique doit exister chez toutes les personnes. Cette formule paraît d'évidence ; elle ne l'est pas. Ainsi, la biométrie rétinienne est-elle compatible avec le port de lentilles de contact mais elle exclut les personnes non voyantes ainsi que les personnes ayant une cataracte défaillante ; les procédés de reconnaissance par l'iris sont moins performants en cas de port de lentilles de contact même si un revendeur français de cette technologie assure que le système qu'il propose fonctionne avec des lunettes de soleil ! La reconnaissance par le contour de la main pose certains problèmes pour les enfants, et la CNIL a été saisie d'un système de contrôles d'accès par le contour de la main au motif que les empreintes digitales de la population concernée, le personnel de nettoyage d'un établissement public, avaient été altérées par les produits détergents...

L'unicité : l'élément biométrique doit être distinct d'une personne à une autre. À cet égard, tous les éléments biométriques ne sont pas équivalents et le taux de discrimination d'une personne à une autre est très différent selon la biométrie en cause. Les éléments biométriques les plus discriminants sont l'ADN, mais aussi la rétine et, bien entendu, l'empreinte digitale. Mais, la reconnaissance par l'iris, moins discriminante que la reconnaissance rétinienne, le serait davantage que l'empreinte digitale. La reconnaissance faciale est considérée comme plus discriminante que la géométrie de la main, la voix ou la signature manuscrite. En tout état de cause, la discrimination est très forte. Ainsi, la probabilité que l'iris d'une personne soit semblable à celui d'une autre personne est de 1 sur 10 alors que la population humaine est d'un ordre de grandeur de 6×10^9 ...

La permanence : la propriété du biométrique doit rester permanente dans le temps pour chaque personne. On pourrait imaginer qu'une telle caractéristique exclut d'emblée certains éléments biométriques, tels que le contour de la main (qui grossit avec les ans), la voix qui s'altère ou le visage qui vieillit. Cependant, les progrès technologiques sont à ce point considérables qu'ils permettent d'anticiper sur

certaines évolutions de l'élément biométrique. Ainsi, les procédés de reconnaissance de visage sont conçus pour identifier des visages de 3/4, d'autres technologies comportent des systèmes d'alerte sur la nécessité de procéder à un nouvel enregistrement de l'élément biométrique de comparaison et un rhume n'altère pas la reconnaissance les procédés de reconnaissance par la voix qui reposent sur les caractéristiques physiologiques de l'appareil phonatoire (c'est-à-dire l'ensemble formé par les poumons, les cordes vocales, la trachée, la gorge, la bouche et les lèvres) plus que sur le son de la voix.

L'accessibilité et la quantifiabilité : est la dernière caractéristique de l'élément biométrique, lequel doit être collectable et mesurable afin de pouvoir être comparé.

La collecte se réalise à l'occasion d'une phase dite « d'enrôlement » que les commerciaux aiment à appeler « la cérémonie d'enregistrement ». La collecte des données primaires (image de l'empreinte, caractéristique de l'iris ou de la rétine, enregistrement de la voix) est opérée au travers d'un capteur spécifique au type de biométrie.

La mesure repose sur ce que les techniciens de la matière appelle le « gabarit » qui est une réduction structurée d'une image biométrique. C'est le gabarit qui se présente sous la forme d'une suite numérique qui va être conservé et non l'élément biométrique lui-même. Ainsi, à partir d'une taille d'images d'un million ou plus d'octets, le gabarit calculé occupe tout au plus quelques milliers d'octets. Ce gabarit est original et spécifique à chaque industriel ou éditeur de technologies biométriques et sa structuration exacte n'est pas destinée à être rendue publique.

Les professionnels concernés font ainsi valoir que l'expression de « fichiers d'empreintes digitales » est impropre, le fichier ne comportant que le gabarit de l'empreinte et non pas l'image de notre doigt. Il s'agit évidemment d'une commodité de langage : on dit généralement « fichier d'empreintes digitales » comme l'on dit « fichier d'empreintes génétiques », expression consacrée par la loi pour désigner le fichier des gabarits d'ADN des personnes condamnées pour certaines infractions.

Dans le même souci de rassurer l'opinion, eu égard à la connotation policière de ces technologies, leurs concepteurs font valoir qu'il est impossible à partir du gabarit de conserver restituer ou de recréer l'image, par exemple, d'un doigt si la technologie est celle de l'empreinte digitale. Cela est vrai mais assez largement indifférent dans la mesure où en appliquant à la trace d'un doigt repérée sur une table ou un verre, l'algorithme utilisé par le concepteur de la base de données, on peut aisément en rapprochant les deux gabarits, savoir si la personne concernée était fichée dans la base et, dans l'affirmative, de qui il s'agit.

2 — LES CARACTERISTIQUES COMMUNES DES SYSTEMES DE RECONNAISSANCE BIOMÉTRIQUE

La performance du système. Elle est mesurable en termes d'erreurs et en vitesse d'identification.

Deux taux d'erreurs sont utilisés pour caractériser le potentiel d'une technique biométrique et la précision d'un système biométrique concret. Le premier taux est celui de la fréquence statistique d'un rejet erroné, c'est-à-dire la non-reconnaissance de quelqu'un qui aurait normalement dû être reconnu. C'est ce que l'on appelle le FFR pour *False Reject Rate.* Le deuxième taux correspond à la fréquence statistique d'une imposture acceptée : le système a reconnu à tort un individu qui n'aurait pas du être accepté. C'est le FAR pour *False Access Rate.* L'optimum de la combinaison des deux taux à leur plus bas (le EER) est l'élément utilisé pour caractériser la performance d'une technique biométrique. Évidemment, ces taux, calculés théoriquement dans des conditions expérimentales, méritent d'être mieux appréciés lorsque le système est mis en oeuvre effectivement. Ainsi, peut-on passer d'un FAR de 0,1 % annoncé commercialement à un FAR beaucoup plus élevé en pratique.

Un autre ajustement de ces taux peut être défini par l'exploitant du système qui préférera diminuer le risque de rejet erroné en préférant admettre une erreur ou, tout au contraire, diminuer le risque d'une acceptation à tort lorsque, par exemple, il en va de la sécurité d'une installation.

Un souci de sécurité ou les performances moyennes d'une technologie pourront parfois conduire l'exploitant du système biométrique à l'associer avec d'autres technologies d'identification ou d'authentification. Ainsi, certains dispositifs pourront cumuler par exemple la reconnaissance du visage et les empreintes vocales. Sur un clavier d'ordinateur, on pourra taper un mot de passe, présenter ses empreintes digitales et introduire une carte à puce. On trouvera alors un triple niveau d'authentification par ce que l'on sait (le mot de passe), par ce que l'on possède (la carte), par ce que l'on est (l'élément biométrique). Cette association de technologie biométrique avec d'autres procédés plus courants de reconnaissance est dénommés la biométrie multimodale. Un exemple de déploiement multimodal se trouve en Israël qui a mis en oeuvre à quarante-deux points de passage de travailleurs journaliers Palestiniens des contrôles d'identité par reconnaissance faciale et géométrie de la main, mémorisées sur une carte à puce.

La tolérance par l'usager. Il s'agit d'un facteur extrêmement important qui fait l'objet d'études qualitatives. À titre d'exemple, le contrôle rétinien qui repose sur les caractéristiques du réseau vasculaire qui forme une image accessible au travers de la pupille avec un appareillage sophistiqué est considéré comme particulièrement incommode. En effet, l'utilisateur doit coller son œil sur un œilleton traversé par un rayonnement infrarouge, évidemment d'une intensité inoffensive. Mais l'enregistrement devient impossible si l'œil est éloigné du lecteur au-delà de trois centimètres. Aussi, cette technologie n'est-elle en pratique utilisée que pour les accès les plus hautement sécurisés. Elle est aujourd'hui mise en œuvre pour certains personnels du FBI et militaires américains, suisses, espagnoles et suédois. En revanche, l'acceptabilité de la reconnaissance par l'iris est bien meilleure dans la mesure où la distance de l'œil au capteur est de l'ordre de 60 centimètres. Aussi, les industriels qui la déploient font-ils valoir que cette technologie est adaptée à la reconnaissance à grande échelle, par exemple, pour contrôler des passagers aériens. Sur ce sujet, une étude menée par Bio Trust en Allemagne est actuellement en cours pour évaluer la tolérance à l'égard de huit technologies différentes.

La robustesse. C'est la qualité qui caractérise la résistance à la falsification ou à l'imposture. Cette question préoccupe naturellement beaucoup les industriels. Ainsi, certains procédés de reconnaissance digitale vérifient-ils le caractère vivant (par la circulation du sang et la chaleur qu'elle dégage) du doigt qui est présenté.

Enfin, la dernière qualité est celle de **l'interfaçabilité** du système avec d'autres systèmes informatiques.

B. Un cas particulier : l'essor de la technologie de la reconnaissance des visages

1 — UNE COURTE HISTOIRE PLEINE DE PROMESSES...

La plupart des articles scientifiques s'accordent à faire remonter à 1973 la première publication scientifique traitant du thème de la reconnaissance du visage, avec l'article du japonais T. Kanade « *Picture processing by computer complex and recognition of human faces ».* Mais le nombre de publications scientifiques traitant de ce sujet ne commence vraiment à décoller qu'à partir de la fin des années 80.

1991 fut un tournant en matière de recherche théorique, avec la publication de l'article intitulé « *eigenfaces for recognition »* de Pentland et Turk, du MIT (Massachusetts Institute of Technology). L'article décrivait un algorithme révolutionnaire, les *« eigenfaces »,* qui eut pour mérite de faire sortir le thème de la reconnaissance du visage du cadre « académique » dans lequel il était resté cantonné jusqu'alors et de permettre de passer à un stade plus « opérationnel ». Pentland et Turk, grâce aux moyens du MIT, pouvaient, en outre, étayer leurs affirmations sur des données expérimentales réelles et significatives.

Le passage vers des produits commerciaux reçut une impulsion décisive à partir des années 1994-1996 grâce à la mise en œuvre du programme FERET *(Face Recognition Technology),* organisé par le ministère de la Défense américaine *(Department of Defense, DoD).* Le nom du service de ce ministère chargé de piloter le projet *(« counterdrug »)* en dit long sur les objectifs assignés à ce programme : « développer des capacités de reconnaissance automatique pour aider au travail des personnels des services de sécurité, d'espionnage... ».

À l'issue de ces tests d'évaluation de 1996, l'ensemble des acteurs du monde de la reconnaissance de visage, laboratoires de recherche mais aussi industriels, disposaient d'une base d'images de référence. Jusque-là en effet, en dehors de la base de données du MIT, chaque laboratoire disposait de sa propre base d'images comprenant tout au plus cinquante individus. La base de données FERET contient 14 126 images pour un total de 1 199 individus. Un individu peut avoir été photographié plusieurs fois, le même jour ou à un intervalle d'un à deux ans, élément précieux pour évaluer l'influence sur les algorithmes de reconnaissance de visage du changement dans l'apparence des individus dû à l'âge, à la coiffure, à l'éclairage, à la posture etc.

Ont pu également être comparés sur des bases objectives des produits totalement différents, mises en évidence les insuffisances ou les limites de chaque algorithme.

Depuis la fin du projet FERET en 1996, le grand changement est l'apparition sur le marché de produits commerciaux. La grande compétitivité du marché a fait éclore un grand nombre d'algorithmes de reconnaissance de visage ou de variantes, dont la plupart n'étaient même pas présents lors des tests d'évaluation FERET, à des prix de plus en plus compétitifs. Aujourd'hui, selon le site Web du ministère de la Défense américaine, « il existe des douzaines de systèmes de reconnaissance du visage qui sont potentiellement capables de satisfaire aux contraintes de performance des nombreuses applications ».

Le ministère de la Défense américaine décida alors de lancer le programme FRVT 2000 *(Facial Recognition Vendor Test 2000)* dont l'objectif était d'évaluer les performances des produits commerciaux.

Ainsi, les techniques de reconnaissance du visage sont non seulement théoriquement viables (c'était le résultat du premier test d'évaluation FERET en 1994) mais un niveau de maturité industrielle paraît désormais atteint.

2 — UN EXEMPLE DE MISE EN ŒUVRE MASSIVE

Le 14 octobre 1998, le *Borough de Newham* de Londres (un quartier populaire à l'est du Grand Londres) mît en service un système destiné à diminuer le nombre de crimes et délits de 10 % en 6 mois, grâce à l'utilisation du logiciel de reconnaissance de visage appelé Mandrake. Le système alertait les opérateurs de caméra dès qu'il y avait 80 % de concordances entre l'image préalablement numérisée d'un délinquant et ce que captaient les caméras. Cent photos de délinquants issues de fichiers appartenant à deux commissariats de police locaux furent numérisées. Le logiciel Mandrake de reconnaissance de visage était installé sur des micro-ordinateurs pour l'analyse des images captées par cent quarante caméras.

Ce projet fut critiqué par le *Data Protection Registrar* (l'homologue de la CNIL en Grande-Bretagne) qui s'inquiétait des menaces sur la vie privée, mais le conseil municipal répondit que le système ne conservait aucune donnée personnelle mais uniquement des photographies et des numéros de référence de la police ! Il fut de même très vivement contesté par de nombreuses associations des Droits de l'homme.

Dix-huit mois après sa mise en œuvre, la municipalité se flattait d'une baisse de la délinquance et le Premier ministre britannique s'est rendu sur place accompagné du ministre de l'Intérieur.

3 — QUELQUES AUTRES APPLICATIONS

Le transport aérien est très intéressé par les technologies de reconnaissance faciale dans la mesure où, intégrées au point de contrôle des passeports, elles permettraient de comparer les photos des passeports avec une base de personnes recherchées.

Le contrôle de certains « grands événements » mobilisateurs de foule sera également, à n'en pas douter, un domaine de prédilection pour l'utilisation de la reconnaissance faciale. Ainsi, lors du *« Super Bowl »* (finale des finales du football américain] qui eut lieu à Tampa en Floride en janvier 2001, les autorités locales ont utilisé la vidéosurveillance associée à la reconnaissance faciale pour surveiller le stade afin de repérer d'éventuels criminels recherchés.

D'autres déploiements récents de la reconnaissance faciale peuvent être cités. Ainsi lors de l'élection présidentielle en Ouganda en mars 2001, chacun des 10 millions d'électeurs se vit attribuer une carte d'électeur à puce comportant le gabarit de leur visage. Lors du vote, le visage de l'électeur était comparé en temps réel par logiciel à celui enregistré dans la carte présentée. L'élimination de la fraude (multiples votes par un même individu) aurait été considérable. Dans le souci de traquer la fraude aux moyens de paiement, une grande chaîne de distribution en Afrique du Sud a attribué une carte à puce aux clients volontaires (au nombre de 1 600 à la fin 2001) contenant leur visage sous forme de gabarit. Lors du passage à la caisse pour un paiement, le visage du client est comparé par logiciel à celui mémorisé dans la carte. Le trafic des faux papiers étant assez répandu dans ce pays, le recours à la biométrie a pu séduire de nombreuses entreprises. Pour le contrôle des 40 000 travailleurs journaliers Palestiniens aux quarante-deux points de passage à la frontière d'Israël, la reconnaissance faciale est utilisée en combinaison avec la géométrie de la main.

Dans ces exemples, le recours à la reconnaissance faciale est justifié par ses promoteurs comme étant peu contraignante pour l'usager qui s'y prête, le taux de reconnaissance pouvant de surcroît être singulièrement élevé, la photographie des visages étant préalablement enrôlée dans un cadre normalisé.

Les tragiques événements du 11 septembre 2001 à New York devraient marquer un nouveau tournant dans l'utilisation à grande échelle de la reconnaissance faciale aux États-Unis, aussi bien dans sa déclinaison « vidéo-surveillance », sur le modèle de celle de Newham, des lieux publics, notamment des aéroports, que pour le contrôle des documents d'identité aux points de passage aux frontières.

4 — UN PEU DE TECHNIQUE

Un procédé de reconnaissance robuste doit pouvoir reconnaître des identités malgré les variations dans l'apparence d'un visage au cours d'une scène. Le visage, qui a trois dimensions, est non seulement soumis à un éclairage très varié en contraste et luminosité, mais peut de surcroît s'inscrire sur un arrière-plan comportant lui-même d'autres visages. Cette forme à trois dimensions, lorsqu'elle s'inscrit sur une surface à deux dimensions, comme c'est le cas d'une image, peut donner lieu à des variations importantes.

Le système de reconnaissance doit également être capable de tolérer des variations dans le visage lui-même. Le visage n'est pas rigide, il peut subir une grande variété de changements dûs à l'expression (joie, peine...), à l'âge, aux cheveux, à l'usage de produits cosmétiques...

Les systèmes de reconnaissance de visage peuvent grossièrement être classés en deux grandes catégories : les méthodes basées sur la reconnaissance des caractéristiques d'un visage humain, d'une part, les méthodes dites globales, d'autre part.

Les méthodes basées sur les caractéristiques du visage recherchent et analysent les éléments caractéristiques d'un visage tels que les yeux, la bouche, le nez, les joues... Après le traitement de chacun de ces éléments, l'ensemble des résultats obtenus est combiné pour procéder à la reconnaissance du visage. On peut par exemple déterminer la géométrie du visage à partir de ces éléments, notamment en calculant les distances les séparant (distance entre les deux yeux, entre les deux joues etc.), leurs proportions respectives comme en anthropométrie. Cette catégorie de méthodes est robuste par rapport aux variations de la position du visage dans l'image.

Les méthodes dites globales, elles, traitent l'image dans son ensemble, sans essayer d'isoler explicitement chacune de ses « régions ». Les méthodes globales utilisent par exemple des techniques d'analyse statistique, d'analyse spectrale etc. La force des méthodes globales tient à ce qu'elles utilisent la totalité des caractéristiques du visage, en ne réservant pas un traitement préférentiel à certaines « régions ». Bien entendu, si nous prenons l'exemple d'une méthode basée sur l'analyse statistique, le « poids » d'un oeil, du nez ou de la bouche dans le résultat final devrait être supérieur à celui d'une tache de rousseur située sur la joue, mais c'est l'analyse statistique des pixels de l'image qui le découvrira « naturellement ». En général, les méthodes globales fournissent de bons taux de reconnaissance, mais nécessitent que le visage soit présenté dans un cadre simple : visage présenté à peu près de face, éclairage régulier, arrière-plan simple. Les performances se dégradent rapidement dès qu'il y a des changements d'orientation du visage, que l'éclairage varie brusquement où que l'arrière-plan est trop chargé.

Pour les produits les plus performants, la qualité de la reconnaissance est relativement insensible aux changements dans l'expression du visage, y compris le clignement des yeux, un air renfrogné ou le sourire. La croissance des barbes et des moustaches est compensée par la collecte d'autres éléments du visage suffisamment redondants et fiables. Le style de la coiffure n'a pas d'influence car les cheveux ne font pas partie des éléments pris en compte dans les calculs.

S'agissant de la posture, une orientation de moins de 10-15° par rapport à la position de face ne provoque aucune dégradation des performances. De 15 à 35 à les performances décroissent. Au-delà de 35°, la reconnaissance n'est pas bonne, mais les visages peuvent toujours être comparés avec d'autres visages tournés d'un même angle tant que les yeux restent clairement visibles.

Certains produits mettent en valeur le fait que les performances ne sont pas diminuées lors de la croissance de l'enfant entre l'adolescence et l'âge adulte.

Pour détecter que la personne ne présente pas à la caméra la photographie d'un visage au lieu du visage lui-même, la présence de caractéristiques géométriques que l'on retrouve dans une photographie est recherchée, comme par exemple la bordure rectangulaire. L'usager peut également être invité à sourire ou à faire un clignement d'oeil. Le test d'un visage « vivant » dure en moyenne deux à trois secondes.

Les principales causes provoquant une erreur de reconnaissance sont : une lumière trop éblouissante sur les lunettes rendant la détection des yeux impossible ; des cheveux longs qui obscurcissent la partie centrale du visage ; un éclairage insuffisant qui surexpose le visage (le noirci) et diminue le contraste ; une résolution trop faible (insuffisance de pixels) de l'image.

Le principe du repérage et du pistage par caméra vidéo est particulièrement redoutable : il consiste d'abord à reconnaître le visage de l'individu puis à le suivre en se basant sur ses caractéristiques géométriques et la texture de sa chair. Le pistage peut se poursuivre même si la personne tourne sa tête, y compris complètement.

5 — UN FUTUR SOUS SURVEILLANCE ?

La technologie de la reconnaissance des visages est présentée par le MIT *(Massachusetts Institute of Technology)* comme une des dix technologies les plus prometteuses pour les dix prochaines années....

Au regard des valeurs de la « loi informatique et libertés », si la technique venait à se développer et ses résultats à s'affiner, deux risques sérieux seraient à redouter.

Le premier serait celui d'un enrichissement de la base de comparaisons, en augmentant considérablement le nombre des photographies des personnes que l'on souhaite rechercher ou surveiller. D'abord limité aux personnes qui sont officiellement recherchées par les autorités publiques, en vertu par exemple d'un mandat d'arrêt, n'y aurait-il pas un risque que l'on recherche ensuite de simples suspects, puis des personnes non suspectes d'avoir commis une infraction mais qui, précédemment connues des services de police, pourraient être placées sous une surveillance permanente afin de contrôler leurs faits et gestes dans le souci de prévenir un comportement délictueux.

Le deuxième risque serait celui d'une augmentation du nombre de caméras de vidéo-surveillance installées dans les lieux publics ou ouverts au public, bref d'un élargissement des périmètres surveillés. Il ne serait d'ailleurs pas, dans une telle hypothèse, nécessaire de conserver les images captées pendant une longue durée, dans la mesure où l'objectif alors poursuivi consisterait moins à exercer une surveillance générale de tous qu'à repérer les lieux où pourraient se trouver des personnes recherchées.

Cumulés l'un à l'autre ces deux risques donnent la mesure des tentations. Il convient à ce stade de relever que lorsqu'un système de vidéosurveillance est couplé à un logiciel de reconnaissance des visages, la loi du 6 janvier 1978 est applicable dans son intégralité, le dispositif ne pouvant être mis en oeuvre par une administration ou une personne morale de droit public qu'après avis favorable de la CNIL. Un tel contrôle n'est pas applicable au secteur privé mais le projet de loi de transposition de la directive, en son état actuel, soumet à un régime d'autorisation tous les traitements de données personnelles incluant des données biométriques. Un tel contrôle préalable par une autorité indépendante est de nature à prévenir le risque d'une

prolifération excessive de cette technologie, sans doute porteuse de sécurité, mais à tous égards redoutable pour nos libertés.

C. La pertinence des instruments juridiques de protection des données à caractère personnel dans la recherche d'un juste équilibre

Incontestablement, les progrès technologiques et la diversité des usages des techniques de reconnaissance ou d'identification biométriques, qu'autorise notamment la baisse des coûts, constitue un puissant facteur de développement et de relative banalisation des contrôles biométriques. Les industriels du secteur s'efforcent parallèlement d'assurer à ces technologies un renouveau, le plus éloigné possible de leurs origines policières ou sécuritaires, en faisant valoir la variété des finalités possibles dépourvues de toute connotation policière ou de recherche des personnes.

Ces efforts destinés à inciter l'opinion à une plus grande tolérance sociale à l'égard de telles technologies sont loin d'être vains et chaque emploi de technologie biométrique à des fins non policières est mis en valeur comme illustration de ces nouvelles tendances, même s'il demeure frappant de constater que les plus grandes applications, en tout cas les applications de masse, se situent plutôt dans l'hémisphère Sud, dans des pays en développement ou plus particulièrement soucieux de leur sécurité intérieure (l'Ouganda, Israël, le Mexique, les Philippines, l'Afrique du Sud sont très fréquemment cités à ce titre).

Cette observation, comme les développements précédents sur la reconnaissance des visages, ne doit nullement donner le sentiment que les autorités de protection des données personnelles entretiendraient une méfiance particulière à l'égard de ces développements technologiques. C'est bien leurs usages et l'idée qu'une société se fait d'elle-même qui doivent être questionnés. À cet égard, on ne peut que constater la grande pertinence des instruments juridiques de protection des données pour rechercher un juste équilibre.

1 — LES PRINCIPES DE PROTECTION DES DONNEES PERSONNELLES APPLICABLES AUX TECHNOLOGIES BIOMÉTRIQUES

Par nature, un élément d'identification biométrique ou sa traduction informatique sous forme de gabarit constitue une donnée à caractère personnel entrant dans le champ d'application des lois « informatique et libertés » comme d'autres données personnelles (un nom, une adresse, un numéro de téléphone, etc.). La finalité de ces techniques consiste en effet, pour l'essentiel, à reconnaître une personne physique, à l'identifier, à l'authentifier, à la repérer.

À cet égard, lorsque le traitement des données biométriques suppose la conservation et le stockage des gabarits, il y a constitution d'une base de données qui relève alors de l'ensemble des dispositions des lois de protection des données au

premier rang desquelles figurent le principe cardinal de finalité et le principe implicite de nos législations qui en est le corollaire : le principe de proportionnalité.

Principe de finalité et base de données

En réalité, le risque qu'une base de données de gabarits puisse être détournée de sa finalité par ceux qui l'ont constituée ou, mise en oeuvre est généralement très faible. Comme le soulignent les professionnels concernés, une base de gabarits mise en place à des fins de contrôle d'accès ou d'authentification présente assez peu d'intérêt : on ne peut pas, à partir du gabarit, reconstituer l'image de l'élément biométrique utilisé ; un élément biométrique est objectif et peu parlant, moins en tout cas que d'autres informations de fond telles que les goûts d'une personne, son taux d'endettement, ou sa nationalité.

Évidemment, le cas des bases de données centralisées à des fins policières ou judiciaires est différent puisqu'y figurer est porteur d'une information. Un nom associé à un gabarit d'ADN dans le fichier national des empreintes génétiques à fins criminelles signifie forcément que la personne a été condamnée pour une infraction grave ou est actuellement recherchée comme auteur supposé d'un crime ou d'un délit sexuel. Pareillement, figurer dans le fichier national des empreintes digitales de la police nationale signifie que la personne a été mise en cause dans le cadre d'une procédure judiciaire. Ces seuls exemples donnent la mesure du critère fondamental de la finalité.

Mais le risque d'un usage des bases de données biométriques à d'autres fins que celles ayant justifié leur création est majeur lorsque l'élément biométrique fait partie de ceux qui « laissent des traces ». Tel est le cas de l'ADN (un cheveu, de la salive sur un mégot, etc.), de l'empreinte digitale qu'on laisse autour de soi dans toutes les circonstances de la vie, ainsi que des visages qui peuvent être captés par des caméras de vidéosurveillance toujours plus nombreuses dans l'espace public et dans l'espace privé. Une société qui favoriserait le développement de bases de données d'empreintes digitales par exemple, offrirait des moyens considérables et nouveaux — au moins dans l'ordre des « possibles » — d'investigations policières sans forcément qu'un tel objectif ait été initialement recherché. Non pas que les bases de données ainsi constituées l'auraient été à des fins policières mais parce que de telles bases de données, apparemment tout à fait anodines, pourraient être utilisées par la police comme élément de comparaison et de recherche dans le cadre de ses investigations.

Les concepteurs de systèmes font valoir sur ce point qu'une telle éventualité est difficile à concevoir dans la mesure où chaque industriel utilise un gabarit qui lui est spécifique et où les bases de données de gabarits d'empreintes peuvent être chiffrées. Mais de telles précautions n'écartent pas tout risque : en effet, les autorités policières sont habilitées à requérir le concepteur de la technologie de communiquer les caractéristiques logicielles du gabarit utilisé ou les clés de déchiffrement de la base. En outre, le fait que chaque base de données serait spécifique et ne concernerait qu'un nombre trop limité de personnes pour être d'une quelconque utilité dans le cadre de recherches policières d'envergure peut ne pas convaincre dans la mesure où plusieurs industriels du secteur utilisent comme argument commercial

l'interopérabilité des bases de données biométriques qu'ils installent, ce qui peut laisser redouter que les éléments techniques présentés comme des garanties ne soient que très provisoires et ne résistent pas aux tentations.

Aussi, fout est-il affaire de mesure et de proportionnalité.

Évidemment, les bases de données d'éléments biométriques ne laissant pas de trace ne soulèvent pas de difficultés de cette nature : une base de données de reconnaissance de la voix, de gabarit d'iris, de rétine ou du contour de la main ne peut en aucun cas être utilisée à d'autres fins que de reconnaissance et d'authentification des personnes qui sont présentes devant le capteur.

En outre, des mesures de sécurité techniques entourant les bases peuvent apporter des réponses adaptées, dans certains cas, à la recherche de cet équilibre. Ainsi, lors de la 18e conférence internationale des autorités de protection des données qui a eu lieu à Ottawa en septembre 1996, un consultant américain avait-il présenté une solution de nature à prévenir tout éventuel usage policier de base de données d'empreintes digitales constituées à d'autres fins, tant cette question est essentielle dans une société de libertés. Il était ainsi préconisé que le gabarit de l'empreinte digitale soit utilisé pour chiffrer l'élément contenu dans la base de données : ainsi, chaque gabarit d'une empreinte ne pourrait-il être déchiffré qu'en présence de l'intéressé auquel l'information biométrique se rapporte. Plaçant le doigt sur un capteur, les caractéristiques de l'empreinte digitale produiraient un gabarit jouant comme clé de déchiffrement ne pouvant se rapporter qu'à une seule empreinte dont le gabarit aurait été chiffré selon les mêmes modalités lors de son enregistrement : la sienne.

Cette solution originale, mais encore prospective, garantirait de manière absolue qu'une base de données constituée à des fins de contrôle d'accès ne puisse pas être utilisée à des fins de police.

Un déploiement des technologies biométriques sans risque social

Les observations qui précèdent amènent à souligner que les technologies biométriques ont un champ considérable de déploiement possible dépourvu de tout risque social, en tout cas à l'égard des libertés individuelles ou publiques ou du respect de la vie privée : tel est le cas lorsque le gabarit de reconnaissance biométrique n'est pas stocké dans une base de données centralisée mais demeure sur soi, inaccessible à tout tiers.

Les applications possibles sont très nombreuses : l'inclusion d'un dispositif de reconnaissance vocale sur un téléphone portable pour empêcher qu'il puisse être utilisé par un tiers, l'utilisation aux mêmes fins des empreintes digitales pour s'assurer que seul son utilisateur pourra accéder à un micro ordinateur, l'inclusion du gabarit de l'empreinte dans la puce d'une carte bancaire permettant, par comparaison d'un doigt que l'on présente dans un lecteur associé au guichet automatique et de l'empreinte figurant dans la puce, de s'assurer que l'utilisateur de la carte est bien son titulaire. L'ensemble de ces applications fait l'objet de nombreuses études de faisabilité par les professionnels concernés sans qu'à aucun moment, en tout cas sur le

terrain des libertés publiques ou de la vie privée, de tels usages soulèvent de vraies difficultés. L'élément biométrique joue alors le rôle d'une clé qui permet d'entrer chez soi !

Le CNIL a eu l'occasion de se prononcer favorablement sur une de ces applications. Il s'agissait d'une expérimentation de vote électronique où les électeurs volontaires étaient munis d'une carte à puce incluant le gabarit de leur empreinte digitale. Ce recours aux technologies biométriques avait pour objet de s'assurer de l'identité de l'électeur et d'établir les listes d'émargement. Aucune base de données des empreintes digitales des électeurs n'était constituée, l'authentification reposant sur la seule comparaison du doigt placé par l'électeur sur un capteur avec le gabarit de son empreinte figurant dans la puce fichée sur la carte.

2— CONVERGENCES ENTRE AUTORITES EUROPEENNES DE PROTECTION DES DONNÉES

Chaque pays européen a sa tradition. Mais incontestablement, la directive européenne du 24 octobre 1995 et sa transposition, réalisée ou en cours, dans l'ensemble des États-membres contribue à la convergence des points de vue. Ainsi, toutes les autorités qui ont eu à être saisies de développements des technologies biométriques font prévaloir le principe de proportionnalité et le principe de finalité.

L'autorité grecque s'est montrée réservée à l'égard des dispositifs de contrôle de la présence des employés par reconnaissance des empreintes digitales mais admet le recours à de tels systèmes pour des installations à des accès réservés.

L'autorité allemande a émis un avis favorable à l'introduction de caractéristiques biométriques sur les pièces d'identité afin de prévenir leur falsification, projet qui a vu le jour après les attentats du 11 septembre 2001, à la condition que les données en cause soient stockées dans la puce de la carte, pour être rapprochées des empreintes digitales de son titulaire, et ne soient pas conservées dans une base de données. Le Parlement allemand devrait être saisi de ce projet compte tenu de son caractère novateur et de son importance.

L'autorité néerlandaise estime pour sa part que lorsque les éléments biométriques ne sont pas conservés dans une base de données mais uniquement stockés sur un objet que l'utilisateur porte sur lui ou qui est à sa disposition exclusive (une carte à puce, un téléphone portable, un ordinateur, etc.), il n'y a pas lieu d'intervenir. Cette position, qui mériterait incontestablement d'être harmonisée au niveau européen, n'est pas très éloignée des observations précédemment faites par la CNIL.

D. Analyse des avis de la CNIL sur le sujet

Il a déjà été précisé que la CNIL s'était prononcé favorablement sur une expérimentation de vote électronique par carte à puce comportant le gabarit de l'empreinte digitale de son titulaire. Le fait qu'aucune base de données, conservant les

empreintes digitales des électeurs n'était constituée a été souligné par la Commission dans sa délibération.

S'agissant des dispositifs reposant sur la constitution de bases de données, il paraît très significatif que la Commission ait donné systématiquement des avis favorables ou n'ait pas formulé de réserve particulière lorsque la base de données était constituée des **gabarits de contour de la main,** élément biométrique qui, à la différence des empreintes digitales, ne laisse pas de trace complète ou repérable sur les objets qui nous entourent. Tel a été le cas d'une reconnaissance biométrique à des fins de contrôle d'accès et des horaires des personnels de nettoyage du musée du Louvre (avis favorable 01-006 du 25 janvier 2001), du contrôle d'accès mis en oeuvre dans une bijouterie (récépissé de déclaration du 12 février 2001), du contrôle des horaires du personnel soignant à domicile des personnes handicapées (même date), du contrôle des horaires du personnel de nettoyage d'un centre commercial à La Défense (récépissé de déclaration délivré en 2002). Ainsi, que la finalité de la base de données ait été le contrôle d'accès ou le contrôle des horaires, la reconnaissance par le contour de la main n'a jusqu'à présent rencontré aucune réserve de la part de la CNIL.

De même la Commission a délivré des avis favorables ou n'a pas formulé de réserve particulière à l'égard de dispositifs de contrôle d'accès reposant sur la constitution de base de données **d'empreintes** digitales **lorsqu'un impératif de sécurité des locaux à protéger était en jeu.** Ainsi d'un contrôle d'accès à des zones hautement sécurisées de la Banque de France (avis favorable 97-044 du 10 juin 1997), de la COGEMA à La Hague, s'agissant de bâtiments de stockage du plutonium (récépissé de déclaration du 17 novembre 2000), des zones de fabrication dans les locaux du groupement carte bleue (récépissé de déclaration du 25 avril 2001), des zones de fabrication de cartes à puce de la SAGEM (récépissé de déclaration du 25 avril 2002).

En revanche, elle a prononcé des avis défavorables ou sous réserve lorsqu'il s'est agi de bases de données d'empreintes digitales à des fins de contrôle d'accès à la cantine d'un collège (avis défavorable 00-015 du 21 mars 2000), ou à l'ensemble des locaux d'une cité académique, seul l'accès à certaines pièces particulières à protéger, notamment celles réservées au stockage des sujets d'examen avant la date des épreuves lui paraissant, dans ce dernier cas, justifier un tel dispositif. Ces deux délibérations ont été prises au motif notamment de l'absence de tout impératif particulier de sécurité qui distinguerait ces locaux de tous les autres et d'une disproportion manifeste entre le dispositif et l'objectif poursuivi.

La Commission s'est prononcée dans un même sens négatif lorsque les bases de données d'empreintes digitales étaient constituées à des fins du contrôle du temps de travail dans une préfecture (avis défavorable 00-057 du 16 novembre 2000), dans une compagnie aérienne (qui a finalement renoncé à mettre en œuvre le dispositif), ou dans une mairie (avis défavorable 02-034 du 23 avril 2002).

Incontestablement ces décisions esquissent une doctrine qui pourrait, à ce stade, être ainsi résumée.

1 — Les technologies de reconnaissance biométrique ne reposant pas sur le stockage des gabarits dans une base de données ne soulèvent pas de difficulté particulière en termes « informatique et libertés », dès lors que le gabarit est conservé sur soi (une carte à puce) ou sur un appareil dont on a l'usage exclusif (un téléphone portable, un ordinateur, etc.) et nulle part ailleurs.

2 — En revanche, lorsqu'une base de données est constituée dans le cadre d'un dispositif d'identification biométrique, l'élément biométrique retenu peut avoir une incidence sur nos libertés et notre vie privée ; tel est le cas lorsque l'élément biométrique retenu « laisse des traces » dans notre vie quotidienne (ADN, empreinte digitale). Dans un tel cas, le contrôle de finalité et de proportionnalité peut conduire à accepter la mise en œuvre de telles bases de données lorsqu'un impératif particulier de sécurité le justifie.

3 —À défaut d'une telle justification particulière, et lorsqu'une base de données de gabarits est constituée, le choix d'un élément biométrique « ne laissant pas de trace », tel que le contour de la main, la rétine, la reconnaissance vocale, etc. devrait être préféré à la prolifération de fichiers d'ADN ou d'empreintes digitales.

Il demeure que loin de tout dogmatisme, la CNIL souhaite poursuivre toute réflexion utile sur le sujet, en liaison avec les professionnels du secteur concerné et ses homologues européens dans le souci de la recherche du meilleur équilibre possible.

E. Quelques réflexions plus générales

Au-delà de la technique, du souhait des professionnels concernés de rendre leurs produits plus attrayants ou de mieux les distribuer, du souci des administrations ou des entreprises de mieux sécuriser leurs locaux et, quelquefois, leurs personnels, les technologies biométriques révèlent trois enjeux qu'on aurait tort de taire, dissimuler ou sous-estimer.

Le premier enjeu qui concerne la CNIL à titre principal, et sans doute quelques autres, est un enjeu au regard de la vie privée et des libertés personnelles lié à la systématisation de la logique des traces, notamment pour l'ADN, les empreintes digitales mais aussi, bientôt si ce n'est déjà, pour nos empreintes vocales ou l'identification par l'odeur, technologie émergente. Avec ces technologies le monde devient une immense mémoire réelle (nos traces), doublé d'un monde virtuel (la recherche et l'identification de nos traces).

Le deuxième enjeu est lié à l'affaiblissement de l'espace public anonyme. Très largement au-delà de la vidéosurveillance, tous les moyens technologiques nomades estompent la distinction jusqu'alors étanche entre les situations dans lesquelles on est anonyme et celles où nous nous identifions (un achat avec carte bancaire, un appel téléphonique que nous passons par un portable). Ainsi d'une situation de liberté à une situation de non-liberté, il y a désormais bien davantage gradation que distinction. Le bracelet électronique placé à la cheville du condamné qui exécute sa peine à domicile n'est que la figure la plus spectaculaire de ce phénomène. Mais les technologies de reconnaissance du visage associées à la

vidéosurveillance soulèvent pour un plus grand nombre de personnes concernées des problèmes de même nature au regard de la liberté d'aller et de venir ou du droit de manifestation sur la voie publique.

Le troisième enjeu est lié à l'aspiration à disposer de plusieurs identités, au moins virtuelles comme en témoigne les usages d'Internet, monde des pseudonymes, qui contribue sans doute à une fragmentation de l'identité numérique. Parallèlement et bien antérieurement, les légitimes réticences à l'égard des interconnexions de fichiers, notamment administratifs, ont encouragé à une fragmentation de l'identité administrative où se niche notre liberté. Mais cette logique de fragmentation, voire de dématérialisation, ne concourt-elle pas à la montée en puissance de l'identité biologique ?

Comme si la tentation de saisir une identité immuable au niveau le plus profond s'alimentait tout à la fois de notre désir de liberté et de nos craintes que l'identité de l'autre soit incertaine.

Chapitre 4

LA PROTECTION DES DONNÉES EN EUROPE ET DANS LE MONDE

Le 21e rapport annuel indiquait que l'an 2000 pourrait être considéré comme une année charnière dans la mondialisation de la protection des données. L'année 2001 n'a fait que confirmer ces vues.

En 2001, tout d'abord, sous l'impulsion des commissaires européens à la protection des données réunis au sein du groupe dit de l'article 29, l'Union européenne a parachevé l'adoption des instruments juridiques destinés à assurer la protection des personnes en cas de flux de données vers des pays tiers *[cf.* les textes correspondants sur http://www.cnil.fr, rubrique « À l'étranger/Flux transfrontières »). Chacun peut, désormais, avoir connaissance de ces instruments : d'une part, la liste des pays dont le niveau de protection est reconnu au plan européen comme adéquat ; d'autre part, des clauses contractuelles types destinées à assurer une telle protection lorsque l'organisme destinataire est établi dans un pays ne l'accordant pas.

Le droit européen de la protection des données à caractère personnel a atteint sa vitesse de croisière et nous sommes entrés dans une période de sécurité juridique où tous les acteurs établis dans l'Union européenne sont en mesure de développer au plan mondial leurs activités économiques tout en assurant aux personnes concernées, de manière simple, un haut degré de protection des données.

Parallèlement, le mouvement législatif a continué à s'étendre hors de l'Union européenne. Ainsi, neuf pays d'Europe centrale et orientale (Chypre, République Tchèque, Estonie, Hongrie, Lettonie, Lituanie, Pologne, Roumanie, Slovaquie) sont désormais dotés d'une législation ; le gouvernement japonais a déposé au printemps 2001 un projet de loi au Parlement ; le Congrès américain a procédé à des auditions en vue d'une éventuelle législation applicable au secteur commercial dans son ensemble ; toujours aux États-Unis, un projet de loi fédérale, applicable aux seules activités en ligne, a par ailleurs été déposé le 18 avril 2002 par le comité du Sénat en charge du commerce, de la science et du transport. En Amérique latine, c'est au tour du Mexique d'examiner un projet de loi générale sur la protection des données.

Enfin, la tenue de la XXIII[e] conférence internationale des commissaires à la protection des données organisée cette année à Paris du 24 au 26 septembre 2001 et à laquelle ont participé des représentants de plus de cinquante Etats a confirmé que des responsables de pays de plus en plus nombreux, quel que soit le niveau de développement du pays concerné, son continent ou son hémisphère, parfaitement conscients des enjeux en cause, sont demandeurs de coopérations en cette matière. En outre, la conférence internationale des commissaires à la protection des données s'est dotée, cette année, de règles qui lui permettront à l'avenir d'adopter des résolutions communes susceptibles d'être rendues publiques au plan mondial.

Après les événements du 11 septembre, cette conférence fut la seule de niveau international au cours de ce même mois. La tenue de plusieurs des sessions, auxquelles participaient non seulement des commissaires à la protection des données mais également des représentants tant d'administrations, d'entreprises que d'associations de défense des Droits de l'homme, notamment en provenance des Etats-Unis, constituait à elle seule une réponse aux conséquences que pouvaient laisser craindre les événements par l'apport d'analyses précises, de réflexions et la nécessité exprimée de modération à l'égard d'une tendance au « tout sécuritaire ».

I. LA RÉGULATION DES FLUX DE DONNÉES PERSONNELLES VERS LES PAYS TIERS

La directive européenne 95/46/CE sur la protection des personnes à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données a établi les bases d'une politique juridique commune destinée à prévenir le contournement de la législation harmonisée dans l'Union européenne à l'occasion des échanges mondiaux. On se reportera à ce sujet notamment au 18[e] rapport annuel de la CNIL, page 120, et aux rapports suivants sur le principe du niveau de protection adéquat des pays tiers destinataires et ses exceptions.

Sur ce point, la Commission européenne a eu recours à la même procédure que celle utilisée les années précédentes pour reconnaître le niveau de protection adéquat de pays dits « tiers ». Tel fut le cas les années précédentes pour la Suisse, la Hongrie et pour le dispositif particulier dit de la « sphère de sécurité », ou *« Safe Harbor »,* auxquelles peuvent adhérer les entreprises américaines[1]. Cette procédure nécessite le recueil de l'avis des commissaires à la protection des données (groupe institué par l'article 29 de la directive) et des États membres (comité dit de l'article 31). Elle a ainsi été appliquée le 20 décembre 2001 *(JOCE* du 4 janvier 2002) par la Commission européenne pour reconnaître le niveau de protection adéquate assuré au Canada dans les secteurs d'activités régis par la loi sur la protection

[1] 20" rapport annuel d'activité de la CNIL, page 200. A ce jour plus de 180 entreprises ont adhéré à ce dispositif, dont Dun et Bradstreet, Hewlet Packard, Intel, et en 2001 Microsoft.

des renseignements personnels et les documents électroniques du 13 avril 2000. Il s'agit des secteurs relevant de la compétence fédérale, notamment des activités de transport aérien, de banques, de stations de radiodiffusion et de télédiffusion, de transport inter-provincial et de télécommunications.

On notera, par ailleurs, que l'Islande et la Norvège, en tant que membres de l'accord économique européen ayant transposé la directive, sont considérés comme assurant une protection équivalente à celle assurée par les États membres de l'Union.

Sous l'impulsion des commissaires européens, la Commission a également adopté en 2001 deux autres décisions qui complètent cette politique. Ces décisions visent à encadrer les flux de données dans les situations où le niveau de protection adéquat du pays destinataire n'est pas garanti. Selon la même procédure que celle prévue pour la reconnaissance du niveau de protection offert par un pays tiers, les décisions concernées portent sur l'adoption de clauses contractuelles types considérées comme garantissant un niveau de protection adéquat pour les flux de données à caractère personnel en cause.

Ainsi, lorsque le pays destinataire n'assure pas un niveau de protection adéquat, les responsables de traitement en cause, l'exportateur établi dans l'Union européenne, et l'importateur établi dans un pays tiers, peuvent procéder de manière simple par contractualisation de la protection au bénéfice des personnes concernées par le transfert de données.

Cette politique ne se distingue pas, dans son objectif et dans sa forme, de celle mise en place par la CNIL de très longue date. Il convient cependant d'en connaître la portée dans le cadre européen qui est désormais le nôtre.

Les autorités nationales de protection des données ne peuvent s'opposer, sauf circonstances exceptionnelles, à un transfert de données vers un pays tiers opéré par application de ces clauses types.

Ces clauses « types » ne sont pas, cependant, exclusives d'autres modalités contractuelles, mais ces dernières doivent être approuvées par l'autorité nationale de contrôle (en France, la CNIL) et être notifiées à la Commission européenne et aux autres États membres.

Enfin, on notera que la déclaration obligatoire auprès de la CNIL des transferts de données vers les pays tiers peut s'effectuer, soit dans le cadre de la déclaration préalable du traitement concerné, assorti du projet de contrat, soit par simple transmission du projet de contrat ou des clauses assorti du numéro d'enregistrement à la CNIL du traitement concerné.

Suivant les conseils des commissaires européens, la Commission européenne a adopté deux séries de clauses contractuelles types correspondant à des transferts de données de nature différente :

— La première décision en date du 15 juin 2001 (*JOCE du 4* juillet 2001)[1], concerne le transfert de données vers un responsable de traitement établi dans un pays tiers (il peut s'agir, par exemple, de données relatives à des salariés d'une

[1] cf. annexe 9 du présent rapport annuel

entreprise multinationale vers la maison mère qui souhaite offrir des possibilités de mobilité aux cadres des filiales du groupe ou de données commerciales en vue d'opérations centralisées). Cette décision offre un cadre commun à ces diverses catégories de flux, chacune des catégories de flux devant cependant faire l'objet d'une annexe descriptive particulière précisant les finalités du transfert, les catégories de personnes concernées, les destinataires etc. (une annexe, par exemple, pour les données relatives à l'emploi, une autre, par exemple, pour les données commerciales).

— La seconde décision en date du 27 décembre 2001 *(JOCE* du 10 janvier 2002)[1], annexée au présent chapitre, concerne la situation plus simple où un responsable de traitement établi en France souhaite sous-traiter certaines opérations de son traitement à une entreprise établie dans un pays tiers.

Les deux séries de clauses adoptées ainsi que les décisions de reconnaissance du niveau adéquat assuré dans un pays tiers sont accessibles dans leur version en français sur le site de la CNIL http://www.cnil.fr, rubrique « À l'étranger/Flux transfrontières ».

II. II. LES TRAVAUX AU SEIN DE L'UNION EUROPÉENNE

Les travaux en matière de protection des données au sein de l'Union européenne se sont poursuivis en 2001 dans les différentes enceintes compétentes.

A. La proposition de modification de la directive 97/66/CE sur la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques

Le Parlement et le Conseil ont poursuivi leurs travaux sur la proposition de juillet 2000 de la Commission visant à modifier la directive 97/66/CE sur la protection de la vie privée et des données à caractère personnel dans le secteur des télécommunications. Il est prévu que cette nouvelle directive soit adoptée à la fin du premier semestre 2002. Les enjeux du nouveau texte, complémentaire à la directive générale 95/46/CE, concernent l'extension de la protection assurée en matière de télécommunications à toute communication électronique.

Dans ce cadre, outre le régime d'utilisation des données de localisation des mobiles, fondé sur le consentement des personnes concernées, les régimes de la protection en matière de prospection par mél et par SMS devraient être fixés. Ces derniers devraient être alignés, du moins selon le souhait du groupe des commissaires européens à la protection des données, sur le régime de la prospection par

[1] Cf. annexe 9 du présent rapport annuel

automates d'appels et par télécopie : leur usage devrait être subordonné au consentement préalable des personnes concernées, compte tenu du caractère très intrusif de ces médias pour la vie privée.

B. Les travaux du groupe des autorités nationales de protection des données réunies au sein du groupe dit de l'article 29

Le groupe est présidé par le Pr. Stefano Rodota, président de la Commission italienne.

L'ensemble des textes adoptés par le groupe ainsi que son rapport annuel sont accessibles sur le site de la CNIL. Les travaux essentiels de cette année sont les suivants.

1 — COOPERATION AVEC LES PAYS D'EUROPE CENTRALE ET ORIENTALE

Le groupe de l'article 29, à l'instar d'autres groupes consultatifs existant au plan européen, a décidé, lors de sa réunion du 13 décembre 2001, et compte tenu des travaux en cours dans l'Union en vue de l'accession des Pays d'Europe centrale et orientale à l'Union, d'accueillir en son sein, à titre d'observateurs, les commissaires à la protection des données de ces pays. La CNIL et d'autres autorités nationales se sont portées volontaires pour des coopérations particulières.

2 — PAYS TIERS

Au titre de sa mission de conseil auprès de la Commission en matière de protection dans les pays tiers, le groupe a rendu deux avis sur le niveau de protection assuré au Canada et en Australie le 26 janvier 2001. À ce jour, l'adéquation du niveau de protection assuré au Canada dans les secteurs privés de compétence fédérale a été reconnue par la Commission. Les discussions avec les autorités australiennes se poursuivent dans la mesure où, notamment, la loi adoptée en Australie en 2000 n'assure pas la protection des étrangers.

3 — APPLICATION HOMOGÈNE DE LA DIRECTIVE

Internet

Au titre de sa contribution à une application homogène de la directive 95/46/CE du 24 octobre 1995, le groupe a poursuivi ses travaux consacrés au contexte de l'Internet. Il a adopté une recommandation importante concernant la collecte de données en ligne le 17 mai 2001[1]. Dans ses grandes options, celle-ci

[1] Cf. annexe 10 du présent rapport annuel.

reprend les préconisations émises de longue date par la CNIL. Cette recommandation devrait permettre de développer une politique commune à vertu tant pédagogique que de contrôle mise en œuvre par les autorités indépendantes de protection des données en Europe auprès des sites dont les responsables sont établis sur leurs territoires. Dans le même temps, sa publication et sa diffusion hors Europe constitue un outil de diffusion de la culture « protection des données » européenne. Elle a ainsi été portée à la connaissance notamment des organismes privés de pays tiers qui contribuent à la promotion de la protection des données au moyen de procédures de labellisation des concepteurs du protocole P3P, élaboré au sein du consortium 3W en charge des standards du web.

Relations de travail

Le groupe a engagé des travaux importants en matière de protection des données dans le domaine des relations salariales. Son premier avis en la matière en date du 13 septembre 2001 (avis n° 8/2001) constitue une interprétation commune de la façon dont les traitements de donnés à caractère personnel dans ce secteur peuvent être analysés au travers des concepts et principes posés par la directive 95/46/CE, qui ne sont pas encore familiers pour tous les acteurs.

Le groupe a, par ailleurs, engagé des travaux plus spécifiques qui devraient aboutir à l'adoption d'une recommandation sur le sujet de la « cybersurveillance » des salariés, qui, à l'heure actuelle, suscite de nombreuses interrogations dans tous les États membres. Le groupe s'appuie, pour cette activité, sur les travaux engagés au plan national. Il s'agit essentiellement, outre ceux de la CNIL, des travaux réalisés par les autorités des Pays-Bas et du Royaume-Uni.

4 — SECURITE, LUTTE CONTRE LA CYBERCRIMINALITÉ ET LE TERRORISME

Le groupe a suivi de très près les travaux engagés au Conseil de l'Europe depuis 1997 pour une convention sur la cybercriminalité. Il a examiné en 2001 en particulier la version rendue publique du projet de convention datée du 20 décembre 2000. Il suit également ceux engagés dans le prolongement des travaux du Conseil de l'Europe par la Commission européenne dans le cadre de sa communication de janvier 2001 au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité ». Cette seconde initiative vise notamment à étendre et intensifier l'harmonisation à laquelle conduit la convention du Conseil de l'Europe signée le 23 novembre 2001. Ces initiatives, cohérentes entre elles, visent à définir de manière commune au plan international certaines infractions pénales, notamment en matière de pornographie (également, concernant l'Union, de propagande raciste et xénophobe qui fait l'objet d'un protocole additionnel à la convention du Conseil de l'Europe), et de fraude informatique et sur les réseaux (comparable à la loi Godfrain en France). Elle vise également à définir des moyens d'enquêtes, de poursuites pénales et à organiser la coopération au plan international.

Le groupe a rendu deux avis sur ces initiatives, les avis n° 8 du 22 mars 2001 et n° 9 du 5 novembre 2001. À ces occasions, le groupe a reconnu le bien fondé de ces initiatives qui, concernant la sécurité des réseaux, concourent à assurer la protection des données personnelles. Par ailleurs, il a pris acte de l'abandon par les rédacteurs du projet de convention du Conseil de l'Europe de l'approche, initialement envisagée, qui aurait conduit à une surveillance permanente et générale de toute la population des internautes par l'enregistrement a priori de leurs agissements sur Internet, une telle mesure ayant été, dans un principe aussi généralement défini, considérée comme disproportionnée dans une société démocratique. Enfin, le groupe a pris acte de l'approche équilibrée de la communication de la Commission européenne. Cependant, il a également souligné le danger résultant de définitions peu claires ou imprécises de diverses incriminations pénales en cause, ainsi que l'insuffisance des garanties dans le cadre des échanges de données personnelles auxquels conduise l'instauration de coopération avec des pays tiers non dotés d'une législation de protection des données à caractère personnel.

Enfin, le groupe a adopté un avis le 14 décembre 2001 sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme et la criminalité[1].

C. Le troisième pilier

Plusieurs faits marquants sont venus jalonner en 2001 l'Activité des autorités de contrôle communes (ACC) Schengen et Europol, dont la mission consiste à garantir la protection des droits des citoyens face aux traitements automatisés à caractère policier mis en oeuvre dans le cadre de chacune des Conventions applicables[2]. Depuis le 1er septembre 2001, les autorités sont assistées par un secrétariat commun indépendant, conformément à la décision du Conseil de l'Union européenne du 27 octobre 2000.

Ainsi, l'ACC Schengen, dont le nouveau président élu en 2001 est M. Giovanni Buttarelli, membre de la délégation italienne, a vu le nombre de pays participant au Système d'information Schengen (SIS) s'élargir, les cinq pays nordiques (le Danemark, la Finlande, l'Islande, la Norvège et la Suède) ayant abandonné depuis le 25 mars 2001 leur statut d'observateur pour devenir des membres actifs de Schengen.

En outre, la situation particulière du Royaume-Uni et de l'Irlande, qui sont les deux seuls pays de l'Union européenne à ne pas appliquer l'accord de Schengen, mais qui ont décidé, comme le permet le protocole Schengen annexé au traité d'Amsterdam, de participer à certaines de ses dispositions, vient singulièrement compliquer l'application des dispositions de la Convention Schengen relatives au SIS. L'ACC a pour tâche de veiller, avec le concours des représentants des autorités nationales de protection des données du Royaume-Uni et de l'Irlande, qui ont la qualité d'observateurs, à ce que la mise en oeuvre du SIS dans ces pays soit conforme à la

1 Cf. annexe 10 du présent rapport annuel.
2 Cf. la Convention d'application de l'accord de Schengen du 19 juin 1990 et la Convention portant création d'Europol du 26 juillet 1995.

décision de leurs gouvernements de ne pas souscrire à l'article 96 de la Convention (non-admission dans l'espace Schengen).

Par ailleurs, dans le prolongement des actions menées afin de parvenir à une meilleure information des citoyens, l'ACC a publié un mémento décrivant les modalités de droit d'accès aux informations enregistrées dans le SIS, destiné à toute personne confrontée, tant à titre professionnel que privé, à l'exercice de ce droit fondamental auprès de l'autorité nationale de protection des données de l'un des pays participant à Schengen.

Enfin, dans la perspective de l'élaboration du SIS II, qui devrait être mis en oeuvre d'ici cinq ans, l'ACC a entamé l'examen des projets des États visant à doter le système Schengen de nouvelles fonctionnalités (extension des signalements enregistrés, nouveaux destinataires de données, etc.), qui devraient vraisemblablement modifier la nature du SIS en accentuant son caractère de fichier de renseignement policier.

L'ACC Europol, présidée par M. Alex Türk, membre de la commission française, a poursuivi ses travaux dont l'essentiel a porté sur la création de nouveaux fichiers d'analyse, les suites de l'inspection effectuée en novembre 2000 et la signature d'accords entre Europol et des pays tiers pour procéder à des échanges de données personnelles.

Les événements du 11 septembre 2001 ont eu des incidences immédiates sur l'activité d'Europol et, par voie de conséquence, sur celle de l'ACC. Ainsi, pour la première fois, le directeur d'Europol a décidé de suivre la procédure exceptionnelle prévue par la Convention Europol et les actes du Conseil de l'Union européenne pris pour son application permettant, en l'absence de tout accord, de transmettre des informations à caractère personnel à un pays tiers, dans le cas d'espèce les Etats-Unis (cf. décision du 28 septembre 2001). Partageant l'avis selon lequel seule la conclusion d'un accord entre Europol et les Etats-Unis serait susceptible de pérenniser des échanges d'informations tout en assurant un niveau de protection des données adéquat, l'ACC et Europol ont depuis lors mis en place une coopération étroite dans le but de garantir la protection des données, quels que soient les défis auxquels les États-Unis peuvent être confrontés.

Le comité des recours, instance chargée aux termes de la Convention Europol d'examiner les recours qui peuvent être formés par les particuliers à la suite d'une demande de droit d'accès aux informations les concernant susceptibles d'être détenues par Europol, a été saisi de deux affaires, en cours d'examen.

2001 fut enfin l'année de l'installation officielle d'une troisième autorité de contrôle commune, l'ACC « Douanes »[1]. Cette instance, qui a élu son président, M. Francis Aldhouse, membre de la délégation du Royaume-Uni, et adopté son règlement intérieur, est désormais opérationnelle. Elle est compétente pour vérifier l'application des dispositions de protection des données à caractère personnel au Système

[1]Cf. 20e rapport d'activité 1999, p. 189

d'information douanier (SID), qui devrait être mis en place par la Commission européenne au cours de l'année 2002.

III. L'ÉTAT DU DROIT DE LA PROTECTION DES DONNÉES DANS LE MONDE

On trouvera en annexe 8 à ce rapport, pays par pays, les références de l'ensemble des législations adoptées à ce jour dans le monde, accompagnées des coordonnées des autorités nationales compétentes. Pour les Etats membres de l'Union européenne et les États de l'accord économique européen, sont mentionnés les textes correspondant à la transposition de la directive 95/46/CE.

De nombreux événements ont marqué l'année 2001 dans le domaine de la protection des données. Parmi ceux-ci, il convient de souligner tout particulièrement l'importance stratégique que représente l'adoption de lois spécifiques de protection des données dans des pays qui étaient, jusque récemment, peu sensibilisés à ces questions, voire réticents. Mais ce panorama général ne doit pas dissimuler une relative disparité dans le niveau de garanties offert, même si le mouvement général en faveur de l'adoption de législations sur le sujet donne à penser que les partisans de mécanismes de protection de la vie privée ne reposant que sur la seule autorégulation par les acteurs professionnels sont de moins en moins nombreux.

On notera tout d'abord qu'en 2001, la Roumanie et Chypre ont adopté des législations sur la protection des données personnelles, ce qui porte à huit le nombre des pays d'Europe centrale et orientale dotés d'une telle protection (outre ces deux pays, la République Tchèque, l'Estonie, la Hongrie, la Lettonie, la Lituanie, la Pologne et la Slovaquie). Les autorités européennes, dont la CNIL, contribuent à la mise en place de ces législations par des missions sur place d'assistance organisées à l'initiative des autorités des pays concernés par la Commission européenne avec son soutien financier (programmes TAIEX et PHARE), et dans la mesure du possible en coopération avec le Conseil de l'Europe.

En Amérique latine, après l'Argentine, le Brésil, le Chili et le Paraguay, c'est au tour du Mexique d'examiner un projet de loi général sur la protection des données visant à compléter certaines mesures sectorielles déjà en vigueur tandis que le Pérou vient de nommer une commission de réflexion chargée d'évaluer la pertinence et l'opportunité d'adopter un texte de portée générale en matière de protection des données personnelles.

Aux États-Unis, l'année 2001 a été marquée par de nombreuses décisions à l'égard de pratiques commerciales estimées contraires aux principes de la protection des données promus soit sur la base de lois sectorielles soit, le plus souvent, sur la base de l'autorégulation. La Commission fédérale pour le commerce *(Federal Trade Commission),* en charge non seulement de la concurrence mais également de la protection des consommateurs, a doublé, après les élections présidentielles, l'effectif de ses services en charge de la protection de la vie privée, et prononcé plusieurs

décisions à l'encontre d'entreprises ne respectant pas notamment la législation relative à la protection de la vie privée des enfants sur Internet.

Par ailleurs, plusieurs décisions de justice sont venues sanctionner de grandes entreprises telle la filiale de Disney, Toysmart, pour la vente illicite de son fichier de clients à l'occasion de sa faillite, ou encore la société Trans Union, une des trois grandes centrales d'informations sur la solvabilité des consommateurs (encours de crédits, revenus etc.), pour détournement de finalité des données recensées à l'occasion de leur communication à des tiers des données à des fins de prospection commerciale.

Au niveau des États, des centaines de projets de loi sont déposés. Dans ce contexte, le congrès se devait d'évaluer la situation générale. La Chambre des représentants a procédé à de multiples auditions en vue de l'examen de l'opportunité de mesures législatives nouvelles, notamment à l'égard du secteur privé qui a suscité de vives réactions de la part de l'industrie et la publication d'études sur le coût jugé exorbitant de la protection des données. Cependant, et malgré les événements du 11 septembre, un groupe de sénateurs républicains et démocrates, appartenant au comité pour le commerce, la science et le transport a déposé le 18 avril 2002 un projet de loi général sur la protection des données collectées en ligne.

Dans la zone Asie-Pacifique, un projet de loi a été adopté par le gouvernement japonais en mai 2001. À Singapour, les autorités encouragent les organisations professionnelles à élaborer un code de déontologie.

On notera, également, les activités importantes qui se sont poursuivies au sein de l'enceinte internationale du Conseil de l'Europe, qui a fêté cette année le 20e anniversaire de la Convention 108.

En effet, un protocole additionnel à la Convention 108 de 1981 sur la nécessité d'instituer des autorités indépendantes de contrôle et de prévoir des garanties en matière de flux transfrontières de données a été ouvert à la signature le 8 novembre 2001. Ces dispositions sont, bien évidemment, compatibles avec les dispositions de la directive 95/46. L'entrée en vigueur de ce protocole additionnel est subordonnée à sa ratification par cinq États. À ce jour, si le protocole a été signé par dix-huit États membres du Conseil de l'Europe, dont douze de l'Union européenne (France incluse), seule la Suède l'a ratifié.

Par ailleurs la convention sur la cybercriminalité (voir ci-dessus le paragraphe sur les activités du groupe dit de l'article 29) a été signée le 23 novembre 2001 par vingt-six États membres et les quatre États non-membres qui avaient participé à son élaboration, l'Afrique du sud, le Canada, les États Unis et le Japon. Elle entrera en vigueur lorsqu'elle aura été ratifiée par cinq États, dont au moins trois du Conseil de l'Europe (http://www.coe.int).

IV. LA 23e CONFERENCE INTERNATIONALE DES COMMISSAIRES À IA PROTECTION DES DONNÉES

La conférence internationale des commissaires à la protection des données est la seule conférence annuelle tenue au plan mondial qui soit exclusivement dédiée à la protection des données personnelles. Elle est organisée chaque année au mois de septembre par une des autorités en charge de la protection des données. Cette année la CNIL fut l'hôte de sa vingt-troisième réunion, qui prit place à la Sorbonne du 24 au 26 septembre 2001.

Cette conférence a réuni plus de 300 personnes de tous les continents. Plus de cinquante pays étaient représentés. La CNIL avait tenu, avec le soutien du Ministère des affaires étrangères, à inviter des personnalités des continents d'Afrique (Burkina Faso, Sénégal, Egypte, Maroc, Mali, Madagascar) et d'Amérique latine (Argentine et Mexique notamment) qui, pour la première fois, étaient représentés par des intervenants ou des délégations de haut niveau à une telle conférence.

Lors de la séance inaugurale, au cours de laquelle M. Jacques Chirac, président de la République a fait lire un message mettant l'accent notamment sur le rôle « crucial » des autorités indépendantes qui « veillent à ce qu'aucune personne, ni publique, ni privée, ne puisse faire un mauvais usage des données personnelles », M. René Blanchet, recteur-chancelier des universités de Paris a prononcé une allocution de bienvenue et le président de la CNIL précisé les enjeux des débats, tout particulièrement après le traumatisme mondial provoqué par les attentats du 11 septembre.

Sous le titre « Vie privée — Droit de l'homme », la CNIL a souhaité donner d'emblée la parole à de « grands témoins » de projets informatiques qui ont marqué l'histoire de la protection des données ces dernières années afin qu'ils fassent part des inquiétudes que ces projets ont suscitées, de la réponse apportée, et du retentissement de l'affaire dans le pays concerné ou au niveau mondial.

Ont été ainsi évoqués au cours de la première session, l'affaire Toysmart aux USA, l'affaire Yahoo ! et la vente d'objets nazis sur un site d'enchères publiques, le programme d'études génétiques sur la population de tout un pays (Islande), l'émergence de la préoccupation de la protection des données à l'occasion d'un projet de carte d'identité au Burkina Faso, le Système français de traitement des infractions constatées (STIC).

La CNIL avait souhaité ensuite que les sauts technologiques auxquels nous assistons ou qui sont activement préparés dans les laboratoires de recherche soient abordés à partir d'une réflexion sur le film *2001, Odyssée de l'espace* de Stanley Kubrick, ses prémonitions et ses erreurs de perspective.

Les sessions consacrées aux questions d'actualité dans tous nos pays, avaient pour orientation centrale l'homme ou la femme dans sa vie quotidienne,

« l'homme situé » comme le disaient certains dans les années 50, citoyen « Cybercrime et cybersurveillance : pour une cybercitoyenneté », « La démocratie électronique », travailleur « Vie privée, vie salariée », patient ou malade « La santé au cœur des fichiers », consommateur « Mouvements d'entreprises, personnalisation des services ».

Ont également été abordés des thèmes centraux face à l'évolution rapide des technologies, « Les biométries et la reconnaissance des visages », « Les techniques de localisation », celui de la pédagogie « Protection des données personnelles et la vie privée : la pédagogie en débat », ou des initiatives prises par les entreprises autour du thème « Entreprises et protection des données personnelles : quelles initiatives et quelle organisation pour assurer la confiance ».

Ces sessions ont permis aux représentants des différents acteurs concernés de confronter au plan mondial leur point de vue, qu'ils proviennent de l'industrie, d'administrations nationales ou d'organisations internationales ainsi que d'associations de défense des libertés. Elles ont été également l'occasion pour les commissaires à la protection des données de mettre en œuvre une de leurs missions fondamentales qui est de faire émerger les questions nouvelles, d'assurer et d'animer le débat public à partir d'informations précises et d'analyses tirées de l'expérience, enfin, de proposer des voies d'arbitrage.

Revenant à une vision plus globale, sous le titre « Un monde, une vie privée », la dernière session donnait la parole à des représentants de différents continents qui ont fait état des progrès réalisés au cours de l'année 2001, notamment en Argentine, aux États-Unis, au Canada, au Japon et dans l'Union européenne.

Enfin, la session réservée aux commissaires à la protection des données a pris une décision importante. En effet, les commissaires ont approuvé des règles d'adoption des résolutions au plan mondial et d'accréditation de ses membres. Il s'est agi de définir les critères permettant à une autorité de disposer du droit de vote : celles dont les textes régissant leurs activités consacrent la protection des données et assurent leur indépendance, qui ont, de plus, des pouvoirs d'intervention effectifs quant à l'assistance qu'elles apportent aux personnes concernées et dont, enfin, les compétences territoriales sont larges. Certains arrangements ont également été fixés pour les Etats à structure fédérale de sorte que les autorités à compétence régionale puissent participer aux travaux de la conférence internationale tout en gardant l'expression d'une seule voix par pays au moment du vote.

Les travaux ont été conclus par M. Lionel Jospin, Premier ministre.

Les textes des interventions effectuées au cours de la conférence sont disponibles en français et en anglais sur le site de la conférence, ainsi que le journal quotidien que la CNIL a pris l'initiative de concevoir durant ces journées sont accessibles sur le site de la conférence (http://www.conference-paris-2001.org). Les actes de la conférence sont publiés à La Documentation française.

ANNEXES

Composition de la Commission au 1er janvier 2002

Président : **Michel GENTOT,** président de section au Conseil d'État

Vice-président délégué : **Hubert BOUCHET,** membre du Conseil économique et social

Vice-président : **Gérard GOUZES,** député du Lot-et-Garonne, maire de Marmande

Commissaires :

Cécile ALVERGNAT, consultant et formatrice NTIC

Maurice BENASSAYAG, conseiller d'État

Didier GASSE, conseiller-maître à la Cour des comptes

François GIQUEL, conseiller-maître à la Cour des comptes

Pierre LECLERCQ, conseiller honoraire à la Cour de Cassation

Philippe LEMOINE, président-directeur général de Laser, membre du directoire des Galeries Lafayette

Jean-Pierre de LONGEVIALLE, conseiller d'État honoraire

Philippe NOGRIX, sénateur de l'Ille-et-Vilaine

Marcel PINET, conseiller d'État honoraire

Guy ROSIER, conseiller-maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social, adjoint au maire de Paris chargé des relations internationales

Alex TÜRK, sénateur du Nord

Alain VIDALIES, député des Landes

Maurice VIENNOIS, conseiller-doyen honoraire à la Cour de Cassation

Commissaires du gouvernement :

Charlotte-Marie PITRAT

Michel CAPCARRERE, adjoint

Répartition des secteurs d'activité

Hubert BOUCHET, vice-président délégué : emploi, recrutement, formation, élections professionnelles

Gérard GOUZES, vice-président : justice (autorité judiciaire, justice administrative, professions judiciaires), autorités administratives indépendantes, Archives nationales

Cécile ALVERGNAT : commerce électronique, plate-forme d'intermédiation, modes de paiement sur Internet

Maurice BENASSAYAG : enseignement public et privé, partis politiques, sondages, marketing politique, droit d'accès indirect

Philippe NOGRIX : banque, bourse, crédit à la consommation

Didier GASSE : marketing, poste, assurance, renseignement commercial, recouvrement de créance, droit d'accès indirect

François GIQUEL : police nationale, gendarmerie nationale, police municipale, renseignement militaire et civil, service national, affaires étrangères, droit d'accès indirect

Pierre LECLERCQ : collectivités locales, recherche médicale, droit d'accès indirect

Philippe LEMOINE : publicité en ligne, télébillétique, localisation des véhicules, veille technologique

Jean-Pierre de LONGEVIALLE : trésor public, fiscalité, cadastre, publicité foncière, douanes, répression des fraudes, comptabilité publique, droit d'accès indirect

Marcel PINET : télécommunications et réseaux, dont Internet (notamment fournisseurs d'accès et d'hébergement, diffusion de données publiques sur Internet), sécurité, cryptologie, participation aux groupes de travail internationaux dans ce domaine, participation au groupe européen dit de « l'article 29 », droit d'accès indirect.

Guy ROSIER : enquêtes statistiques mises en œuvre par l'INSEE, culture, jeunesse et sport, tourisme, logement, immobilier, transport, équipement, environnement, industrie, énergies, artisanat, agriculture, droit d'accès indirect

Pierre SCHAPIRA : aide sociale, action sociale, revenu minimum d'insertion

Alex TÜRK : coopération européenne et internationale en matière de police, justice et douanes, presse, églises, associations, syndicats

Alain VIDALIES : santé : hôpitaux, prévention, réseaux de soins, fichiers des professions de santé, sites web médicaux

Maurice VIENNOIS : sécurité sociale, assurance vieillesse, assurance maladie, allocations familiales, mutuelles, droit d'accès indirect

Organisation des services au 1er juin 2002

Président : **Michel GENTOT**

Secrétaire général, chargé des affaires juridiques : **Joël BOYER,** magistrat

Annexe 4

Liste des délibérations adoptées en 2001

Les délibérations sont publiées dans les chapitres du rapport, à la suite des commentaires qui les évoquent ou en annexe 5. Elles sont signalées dans le tableau suivant, par un renvoi à la page concordante dans le rapport. Le texte intégral de l'ensemble des délibérations de la CNIL, depuis 1978, est accessible par minitel sur le « 3617 jurifrance » ou après abonnement sur le « 3613 JRF », ou par Internet, après abonnement, sur les sites www.jurifrance.com et www.lamyline.com.

Numéro Date	Date et objet
01-001 16 janvier 2001	Délibération décidant un contrôle sur place
01-002 16 janvier 2001	Délibération portant avis sur le projet d'arrêté municipal de la ville d'Issy-les-Moulineaux concernant la mise en oeuvre expérimentale d'un dispositif destiné à diffuser sur Internet des images d'une crèche municipale
01-003 25 janvier 2001	Délibération portant avis sur le projet d'arrêté modifiant l'arrêté du 29 juillet 1998 portant création d'un traitement automatisé par lecture optique des bulletins du recensement général de la population de 1999
01-004 25 janvier 2001	Délibération portant avis sur un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part la gestion des demandes présentées en application du décret n° *2000-657* du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites et d'autre part le paiement des indemnités en capital et des rentes viagères servies sur la base dudit décret
01-005 25 janvier 2001	Délibération relative à un projet de décret portant application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers mis en oeuvre pour l'application du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites

Numéro Date	Date et objet
01-006 25 janvier 2001	Délibération portant avis sur un projet de décision présenté par l'établissement public du Musée du Louvre concernant un traitement de contrôle des accès et des horaires de certains personnels par la reconnaissance du contour de la main
01-007 8 février 2001	Délibération portant désignation de Monsieur Jean-Pierre de Longevialle en qualité de membre de la Commission nationale de l'informatique et des libertés chargé d'exercer le droit d'accès indirect en application de l'article 39 de la loi du 6 janvier 1978
01-008 8 février 2001 (cf. p. 125)	Délibération concernant les modifications apportées pour 2001 par la direction générale des impôts à la procédure de transmission par Internet des déclarations de revenus
01-009 22 février 2001	Délibération portant avis sur le projet de décision portant création d'un fichier des enquêtes au sein du service de l'inspection de la Commission des opérations boursières
01-010 22 février 2001	Délibération décidant un contrôle sur place
01-011 8 mars 2001	Délibération portant adoption d'une recommandation sur les sites de santé destinés au public
01-012 8 mars 2001	Délibération portant avis sur un projet de décision présenté par l'association pour la bonne coordination médico-chirurgicale concernant la mise en place d'un réseau ville-hôpital destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients bénéficiant d'une prise en charge médico-chirurgicale.
01-013 8 mars 2001	Délibération portant avis sur un projet de décision présenté par l'Association Intégrale Santé concernant la mise en place d'un réseau de soins dans la région de Lens destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients
01-014 8 mars 2001	Délibération portant avis défavorable sur le traitement automatisé d'informations nominatives mis en œuvre par La Poste dans le cadre d'une expérimentation dite « Référentiel des boîtes aux lettres »

Numéro Date	Date et objet
01-015 20 mars 2001 **(cf. p. 87)**	Délibération portant avis sur un projet d'avenant à l'accord du 28 octobre 1960 modifié le 28 septembre 1987 conclu entre la direction des archives de France et la société généalogique de l'Utah
01-016 20 mars 2001	Délibération portant avis sur l'avant-projet de loi présenté par l'INSEE concernant la réforme du recensement de la population
01-017 3 avril 2001	Délibération portant avis favorable sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives issues de la base image « Adresse de logement » créée lors du recensement général de la population 1999
01-018 3 mai 2001	Délibération portant avis sur le projet de loi sur la société de l'information
01-019 15 mai 2001	Délibération relative à un projet d'arrêté portant création d'un traitement informatique de délivrance des visas dans les postes diplomatiques et consulaires mis en œuvre par le ministère des Affaires étrangères
01-020 15 mai 2001	Délibération portant avis conforme sur le projet de décret en Conseil d'État autorisant la création par le ministre de l'Intérieur d'un fichier des élus et candidats aux élections au suffrage universel et portant application des dispositions du 3e alinéa de l'article 31 de la loi du 6 janvier 1978
01-021 15 mai 2001	Délibération relative à une demande d'autorisation présentée par l'Institut de veille sanitaire concernant la constitution d'un système national d'information sur le cancer
01-022 15 mai 2001	Délibération décidant un contrôle sur place
01-023 15 mai 2001	Délibération décidant un contrôle sur place
01-024 15 mai 2001	Délibération décidant un contrôle sur place
01-025 15 mai 2001	Délibération décidant un contrôle sur place

Numéro Date	Date et objet
01-026 31 mai 2001	Délibération décidant un contrôle sur place
01-027 31 mai 2001	**Délibération décidant un contrôle sur place**
01-028 31 mai 2001	Délibération décidant un contrôle sur place
01-029 31 mai 2001	Délibération décidant un contrôle sur place
01-030 31 mai 2001	Délibération décidant un contrôle sur place
01-031 31 mai 2001	Délibération décidant un contrôle sur place
01-032 31 mai 2001	Délibération décidant un contrôle sur place
01-033 31 mai 2001	Délibération décidant un contrôle sur place
01-034 31 mai 2001	Délibération décidant un contrôle sur place
01-035 31 mai 2001	Délibération décidant un contrôle sur place
01-036 31 mai 2001	Délibération décidant un contrôle sur place
01-037 12 juin 2001 (cf. p. 118)	Délibération relative à la mise en place de procédures dématérialisées de déclaration et de règlement en matière de TVA
01-038 12 juin 2001	Délibération portant avis sur un projet d'arrêté présenté par le ministre de la Justice portant création d'un traitement relatif à la gestion des procès-verbaux d'infractions de travail illégal destiné à être mis en œuvre dans les comités opérationnels de lutte contre le travail illégal (COLTI)

Numéro Date	Date et objet
01-039 28 juin 2001	Délibération décidant une mission d'investigation destinée à identifier le responsable d'un traitement automatisé d'informations nominatives en infraction avec la loi du 6 janvier 1978
01-040 28 juin 2001 **(cf. p. 42)**	Délibération relative à la mission de vérification sur place effectuée auprès de Canal +
01-041 10 juillet 2001 **(cf. p. 25)**	Délibération portant avis sur le projet de loi de modernisation du système de santé
01-042 10 juillet 2001 **(cf. p. 91)**	Délibération portant dénonciation au parquet d'une infraction à la loi du 6 janvier 1978
01-044 4 septembre 2001	Délibération portant avis sur un projet de décret en Conseil d'État relatif à l'utilisation du RNIPP et sur un projet d'arrêté interministériel concernant la réalisation d'un échantillon inter-régimes d'allocataires de minima sociaux par la direction de la recherche, des études, de l'évaluation et des statistiques du ministère de l'Emploi et de la Solidarité
01-045 4 septembre 2001	Délibération décidant un contrôle sur place
01-046 18 septembre 2001	Délibération portant avis sur un traitement automatisé de constitution des listes électorales prud'homales en vue du scrutin du 11 décembre 2002
01-047 18 septembre 2001	Délibération portant avis sur un traitement sur les fichiers des électeurs inscrits sur les listes électorales prud'homales de 1997, versées aux Archives nationales, à des fins statistiques et d'études présenté par le ministère de l'Emploi et de la Solidarité
01-048 18 septembre 2001	Délibération relative au projet de décision du comité des établissements de crédit et des entreprises d'investissement portant création d'un fichier des dirigeants et actionnaires des établissements de crédit et des entreprises d'investissement dénommé « FIDEC »
01-049 18 septembre 2001	Délibération relative au projet de décret du premier ministre modifiant l'article R. 79 du code de procédure pénale relatif au casier judiciaire

Numéro Date	Date et objet
01-050 10 juillet 2001	Délibération concernant la demande d'avis présentée par France Télécom relative à la présentation systématique aux services d'urgence du nom et de l'adresse correspondant au numéro de la ligne appelante
01-051 9 octobre 2001	Délibération relative aux échanges d'informations mis en place entre la direction générales des impôts et les chambres de métiers
01-052 18 octobre 2001	Délibération portant avis sur deux projets d'arrêtés présentés par le ministre de la Justice modifiant les arrêtés des 18 juin 1986 et 13 avril 1993 relatifs à la mise en œuvre, dans les tribunaux de grande instance, d'un système de gestion automatisée des procédures
01-053 18 octobre 2001	Délibération portant avis sur une expérimentation du Conseil national d'information géographique relative à la faisabilité d'un fichier national de référence de « points géographiques à l'adresse »
01-054 18 octobre 2001 (cf. p. 67)	Délibération portant avis sur le projet d'arrêté présenté par le ministère de l'Emploi et de la Solidarité relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie (SNIIRAM)
01-055 25 octobre 2001 (cf. p. 136)	Délibération relative à la création d'une procédure de transfert de données fiscales pour le compte de l'Etat et des organismes de protection sociale visés à l'article L. 152 du Livre des procédures fiscales
01-056 13 novembre 2001	Délibération relative au projet d'arrêté présenté par la mairie de Paris portant création d'un traitement ayant pour finalité le suivi des candidatures et la gestion administrative du Conseil de la citoyenneté des parisiens non communautaires
01-057 29 novembre 2001 (cf. p. 77)	Délibération portant recommandation sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence
01-058 11 décembre 2001	Délibération portant avis favorable sur le projet d'arrêté présenté par l'INSEE, portant sur la diffusion des résultats du RGP 1999 et modifiant l'arrêté du 22 mai .1998

Numéro Date	Date et objet
01-059 20 décembre 2001	Délibération décidant un contrôle sur place
01-060 20 décembre 2001	Délibération décidant un contrôle sur place
01-061 20 décembre 2001 **(cf. p. 51)**	Délibération portant recommandation relative aux fichiers de gestion du patrimoine immobilier à caractère social
01-062 20 décembre 2001	Délibération modifiant la norme simplifiée n° 20 concernant les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social
01-063 13 novembre 2001	Délibération décidant un contrôle sur place

Annexe 5

Délibérations adoptées en 2001, non publiées dans les chapitres du rapport

Délibération n° 01-002 du 16 janvier 2001 portant avis sur le projet d'arrêté municipal de la ville d'Issy-les-Moulineaux concernant la mise en œuvre expérimentale d'un dispositif destiné à diffuser sur Internet des images d'une crèche municipale

(Demande d'avis n° 728268)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis d'un projet d'arrêté du maire de la ville d'Issy-les-Moulineaux ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 modifié pris pour son application ;

Après avoir entendu Monsieur Pierre Schapira en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Commission nationale de l'informatique et des libertés est saisie par la ville d'Issy-les-Moulineaux d'une demande d'avis concernant l'expérimentation pour une durée d'un an, au sein d'une crèche municipale, d'un dispositif de caméras reliées à Internet permettant aux parents, en se connectant au site Web de la ville, d'observer les activités de leur enfant à certains moments de la journée.

Ce projet, qui est présenté comme s'inscrivant dans le cadre d'une politique locale de développement des nouvelles technologies de l'information, a pour objet de permettre aux parents, au moyen d'un support de communication moderne, d'avoir connaissance en temps réel des actions pédagogiques et des animations réalisées par la crèche.

La mise en place, au sein de structures éducatives telles que les crèches, de ce type de dispositifs, qu'autorise désormais le développement des technologies, offrant aux parents et au personnel d'encadrement la possibilité de veiller sur l'activité et le comportement des enfants et des personnels, appelle incontestablement à une vigilance particulière dans la mesure où leur généralisation ou certains de leurs usages ne sont pas insusceptibles d'avoir des incidences sur l'épanouissement de la personnalité des enfants ou de favoriser un nouveau mode de contrôle de l'activité des personnels.

Il y a lieu dès lors pour la Commission d'apprécier, au cas par cas, si les conditions de mise en oeuvre de tels systèmes sont proportionnées à l'objectif poursuivi.

La Commission observe à cet égard que le projet de la ville d'Issy-les-Moulineaux a une finalité limitée dans la mesure où, outre la directrice de la crèche et la responsable municipale de la petite enfance, seuls les parents pourront accéder aux images de leurs enfants, et ce, de manière ponctuelle.

Elle prend acte que le dispositif est placé sous le contrôle de la directrice de la crèche qui seule déterminera l'orientation et le niveau de zoom des caméras, ainsi que, à l'initiative des membres de l'équipe pédagogique, les plages horaires de diffusion des images et les animations susceptibles d'être ponctuellement filmées. En outre, les personnes seront alertées en temps réel du moment où elles seront filmées par la mise en œuvre d'un procédé d'alerte visuel de sorte qu'en aucun cas elles ne puissent l'être à leur insu.

Aucune conservation des images, qui seront de surcroît chiffrées lors de leur transmission via Internet, ne sera opérée au niveau de la crèche et des services municipaux.

Enfin, la mairie prévoit que les parents seront informés de la mise en œuvre du dispositif et seront invités à donner leur autorisation écrite à la diffusion des images de leur enfant.

Cette garantie doit être étendue aux membres du personnel dans la mesure où les images des personnels concernés seront accessibles aux parents, avec lesquels ils n'ont aucun lien de subordination. Aussi leur consentement exprès devra-t-il être recueilli et les notes d'information à l'attention des personnes concernées devront-elles être complétées pour préciser que la directrice de la crèche et la responsable municipale de la petite enfance seront également destinataires des images.

Enfin, le dossier de demande d'avis de la mairie d'Issy-les-Moulineaux et les projets de note d'information précisant que le système pourra être mis en œuvre, dans les conditions définies ci-dessus, lors de « manifestations publiques », il y aura lieu, afin d'éviter toute équivoque dans l'esprit des personnes concernées sur sa finalité réelle, de préciser cette expression, comme cela a été fait dans le dossier de demande d'avis, en ajoutant qu'il ne pourra s'agir que d'initiatives liées à l'activité de la crèche telles que des activités musicales, des récitations, etc.

Compte tenu de l'ensemble de ces caractéristiques (accès réservé aux parents et limité à certaines plages horaires sous le contrôle de la directrice de la crèche, absence de conservation des images par le dispositif, sécurisation des transmissions des images, autorisation expresse des parents et des personnels de la crèche) et sous ces réserves, la mise en œuvre à titre expérimental de ce projet par la ville d'Issy-les-Moulineaux est proportionnée à l'objectif poursuivi. Eu égard à l'intérêt que pourrait susciter cette initiative, à son caractère expérimental, et à l'éventualité de sa généralisation ou de son extension, la CNIL souhaite qu'un bilan lui soit adressé à l'issue de la période expérimentale.

Compte tenu de ces observations, la Commission :

Émet un avis favorable au projet d'arrêté présenté par la ville d'Issy-les-Moulineaux et portant création, à titre expérimental pour une durée d'un an, d'un traitement automatisé d'informations nominatives permettant aux parents d'enfants de la crèche « La Farandole » de voir leurs en-

fants sur Internet lors d'ateliers pendant des tranches horaires déterminées, **sous réserve** que :
— l'autorisation expresse des personnels de la crèche et des parents soit re cueillie ;
— les notes d'information à destination des parents et des personnels men tionnent l'ensemble des destinataires des images ;
— **demande** à être saisie d'un bilan au terme de l'expérimentation qui doit s'achever au plus tard un an après la notification de la présente délibé ration.

Délibération n° 01-003 du 25 janvier 2001 portant avis sur le projet d'arrêté modifiant l'arrêté du 29 juillet 1998 portant création d'un traitement automatisé par lecture optique des bulletins du recensement général de la population de 1999

(Demande d'avis n° 588086 VI)

La Commission nationale de l'informatique et des libertés ; Saisie pour avis du projet d'arrêté par le ministre de l'Économie, des Finances et de l'Industrie ;

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

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu l'arrêté du 22 mai 1984 définissant l'échantillon démographique permanent de l'INSEE et les dispositions prises pour assurer la sécurité des traitements ;

Vu l'arrêté du 15 juillet 1993 portant création d'un traitement, par scannérisation, de documents issus du recensement de la population de 1990 ;

Vu l'arrêté du 22 mai 1998 portant création d'un traitement automatisé réalisé à l'occasion de la collecte et de la diffusion des résultats du RGP de 1999 ;

Vu l'arrêté du 29 juillet 1998 portant création d'un traitement automatisé par lecture optique des bulletins du recensement général de la population de 1999 ;

Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'INSEE a saisi la Commission nationale de l'informatique et des libertés d'un projet d'arrêté portant modification de l'arrêté susvisé du 29 juillet 1998 créant un traitement automatisé en vue de l'acquisition sur support informatique des images des bulletins du recensement, et de la constitution par saisie ou reconnaissance automatique de caractères, à partir des images des bulletins de trois bases d'images (la base « nom — prénoms — nais sance », la base « adresse de logement », la base « complète non nominative »).

La modification envisagée concerne d'une part, le contenu de la base image « nom — prénoms — naissance » et celui de la base image « adresse de logement » (article 3 de l'arrêté initial), d'autre part, la durée de conservation de la base « nom — prénoms — naissance » (article 6 du même arrêté).. L'INSEE vise à compléter la base « nom — prénoms — naissance » par la date de naissance des personnes, et la base « adresse de logement » par le nom du ménage résidant dans le logement à la date du recensement, données omises lors de la rédaction de l'arrêté susvisé de 1998 ;

Ces ajouts sont justifiés par la finalité des deux bases considérées. La première a en effet pour objet la mise à jour de l'échantillon démographique permanent (EDP) qui ne concerne que les personnes nées entre le 1er et le 4 octobre de chaque année. La seconde base permet la constitution de l'échantillon maître des logements lequel comporte le nom de l'occupant du logement.

L'INSEE demande également que la durée de conservation de la base « nom — prénoms — naissance » soit prolongée d'un an soit jusqu'à la fin 2002. Des retards de mise en œuvre du traitement par lecture optique des bulletins du recensement ne permettent pas à l'INSEE de constituer et d'exploiter ladite base dans les délais initialement prévus.

Au bénéfice de ces observations, la Commission émet un avis favorable au projet d'arrêté qui lui est soumis.

Délibération n° 01-004 du 25 janvier 2001 portant avis sur un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part la gestion des demandes présentées en application du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites et d'autre part le paiement des indemnités en capital et des rentes viagères servies sur la base dudit décret

La Commission nationale de l'informatique et des libertés ; Saisie par le Premier ministre d'un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part la gestion des demandes présentées en application du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites et d'autre part le paiement des indemnités en capital et des rentes viagères servies sur la base dudit décret ;

Vu la Convention 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 modifiée relative à l'informatique, aux fichiers et aux libertés et son décret d'application ;

Vu le décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites ;

Après avoir entendu Monsieur François Giquel, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

La Commission a été saisie par le Premier ministre d'un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part la gestion des demandes présentées en application du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites et d'autre part le paiement des indemnités en capital et des rentes viagères servies sur la base dudit décret.

Aux termes du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites, toute personne dont la mère ou le père a été déporté à partir de la France dans le cadre des persécutions antisémites durant l'Occupation et a trouvé la mort en déportation a droit à une mesure de réparation, qui prend la forme d'une indemnité ou d'une rente viagère, si elle était mineure de vingt et un ans au moment où la déportation est intervenue. Les personnes qui perçoivent une indemnité viagère versée par la République fédérale d'Allemagne ou la République d'Autriche à raison des mêmes faits ne peuvent toutefois bénéficier de cette mesure. La décision accordant ou refusant la mesure de réparation est prise par le Premier ministre, sur proposition du ministre de la Défense. Le projet de décret soumis à l'avis de la Commission a pour objet de créer deux traitements automatisés d'informations nominatives.

Le premier traitement automatisé, qui sera mis en oeuvre par la direction des statuts, des pensions et de la réinsertion sociale du ministère de la Défense, permettra d'assurer l'instruction des demandes de rente viagère ou d'indemnité en capital. Le second traitement, qui sera mis en œuvre par l'Office national des anciens combattants et victimes de guerre, permettra d'assurer le paiement des indemnités accordées.

Sur le traitement automatisé d'informations nominatives ayant pour finalité l'instruction des dossiers de demande

Ce traitement sera mis en œuvre par la direction des statuts, des pensions et de la réinsertion sociale du ministère de la Défense, chargée, aux termes du décret du 13 juillet 2000, de recevoir les dossiers de demande d'attribution d'une mesure de réparation.

Les informations enregistrées portent sur l'état civil et le domicile du demandeur (nom, prénoms, date et lieu de naissance, adresse), les éléments permettant de vérifier que celui-ci remplit les conditions fixées par le décret du 13 juillet 2000 (lien de filiation avec la personne disparue en déportation,

déportation depuis le territoire français, motif de la déportation, âge du demandeur lors de la déportation de ses parents ou de l'un d'eux, attestation de non versement d'une indemnité viagère par la République fédérale d'Allemagne ou la République d'Autriche), et les données utiles pour verser la mesure de réparation en cas de décision favorable du Premier ministre (choix de l'indemnité en capital ou de la rente viagère, relevé d'identité bancaire).

Compte tenu des précisions apportées lors de l'instruction du dossier concernant la finalité et les modalités d'enregistrement dans le traitement des informations permettant de vérifier que les conditions d'attribution d'une mesure de réparation sont remplies par le demandeur, la Commission estime que les rubriques 5 à 9 de l'article 2 du projet de décret devraient être modifiées au vu de la rédaction du décret du 13 juillet 2000 et être rédigées comme suit :

5) personne disparue en déportation : père ou mère du demandeur ;
6) déportation à partir de la France ;
7) déportation dans le cadre des persécutions antisémites durant l'Occupation ;
8) demandeur mineur de vingt et un ans au moment où la déportation est intervenue ;
9) attestation sur l'honneur de non versement d'une indemnité viagère de la part de la République fédérale d'Allemagne ou de la République d'Autriche à raison des mêmes faits.

Le traitement prévoyant l'enregistrement d'informations concernant des personnes demandant à bénéficier de la mesure de réparation prévue par le décret du 13 juillet 2000, un projet de décret portant application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 aux fichiers mis en oeuvre pour l'application de ce décret est soumis à l'avis de la Commission.

Les informations seront conservées trois ans à compter de la date de la décision du Premier ministre, qui, aux termes de l'article 4 du décret du 13 juillet 2000, doit intervenir dans un délai de quatre mois dès lors que le dossier de demande est complet.

Les destinataires des informations seront les agents de la direction des statuts, des pensions et de la réinsertion sociale du ministère de la Défense, et du secrétariat général du Gouvernement chargés d'assurer l'instruction des demandes, habilités nominativement par arrêté du Premier ministre. Le droit d'accès s'exercera en application de l'article 34 de la loi du 6 janvier 1978 auprès du directeur des statuts, des pensions et de la réinsertion sociale du ministère de la Défense, ce dont les personnes seront informées aux termes des documents constituant le dossier de demande qui comportent les mentions de l'article 27 de la loi du 6 janvier 1978.

Sur le traitement automatisé d'informations nominatives ayant pour finalité le paiement des mesures de réparation

Ce traitement sera mis en œuvre par l'Office national des anciens combattants et victimes de guerre (ONACVG), établissement public placé sous la tutelle du ministre de la Défense, chargé, aux termes du décret du 13 juillet 2000, d'assurer le paiement des rentes viagères et des indemnités en capital dès lors que la décision du Premier ministre sera favorable. Seules les informations nécessaires au paiement des indemnités seront transmises par la direction des statuts, des pensions et de la réinsertion sociale du

ministère de la Défense à l'Office national **dus** anciens combattants et victimes de guerre. Il s'agira des nom, prénoms, date et lieu de naissance, adresse, relevé d'identité bancaire du demandeur, des numéros des décisions prises par le Premier ministre, des modalités de versement des indemnités, des montants versés et des dates de versement et numéros de dossiers attribués par l'Office national des anciens combattants et victimes de guerre. Les informations enregistrées seront conservées quatre ans après la date du paiement de l'indemnité en capital ou de la date du virement de la dernière mensualité de la rente viagère.

Les destinataires des informations seront les agents de l'Office national des anciens combattants et victimes de guerre chargés d'assurer le paiement des indemnités en capital et des rentes viagères sur le fondement du décret du 13 juillet 2000.

Le droit d'accès aux informations s'exercera directement auprès du directeur général de l'Office national des anciens combattants et victimes de guerre.

Prend acte de ce que les services du Premier ministre ne mettront en oeuvre aucun traitement automatisé d'informations nominatives dans le cadre de cette procédure, la transmission des informations par la direction des statuts, des pensions et de la réinsertion sociale du ministère de la Défense aux services du Premier ministre s'effectuant sur support papier ;

Au bénéfice de ces observations, émet un avis favorable sur le projet de décret dont elle a été saisie par le Premier ministre, sous réserve que les rubriques 5 à 9 de l'article 2 de ce texte soient rédigées comme suit :

5) personne disparue en déportation : père ou mère du demandeur ;
6) déportation à partir de la France ;
7) déportation dans le cadre des persécutions antisémites durant l'Occupation ;
8) demandeur mineur de vingt et un ans au mornent où la déportation est in tervenue ;
9) attestation sur l'honneur de non versement d'une indemnité viagère de la part de la République fédérale d'Allemagne ou de la République d'Autriche à raison des mêmes faits

Délibération n° 01-005 du 25 janvier 2001 relative à un projet de décret portant application des dispositions du troisième alinéa de l'article 31 de a loi n° 78-17 du 6 janvier 1978 aux fichiers mis en œuvre pour l'application du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites

La Commission nationale de l'informatique et des libertés ;

Saisie par le Premier ministre d'un projet de décret portant application des dispositions du troisième alinéa de l'article *3]* de la loi n° 78-17 du 6 janvier 1978 aux fichiers mis en œuvre pour l'application du décret n° 2000-657 du 13 juillet 2000 instituant une messure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites ;

Vu la Convention 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 modifiée relative à l'informatique, aux fichiers et aux libertés et son décret d'application ;

Vu le décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites ;

Après avoir entendu Monsieur François Giquel, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Commission est saisie pour avis par le Premier ministre d'un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part la gestion des demandes présentées en application du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites et d'autre part le paiement des indemnités en capital et des rentes viagères servies sur la base dudit décret.

Ces deux traitements devant comporter des informations nominatives relatives aux personnes qui, remplissant les conditions prévues par le décret du 13 juillet 2000, demanderont à bénéficier de la mesure de réparation prévue par ce décret, les fichiers envisagés entreront dans le champ d'application de l'article 31 de la loi du 6 janvier 1978.

Aux termes de l'article 31 de la loi, la collecte et le traitement des informations nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs des personnes sont interdits sauf accord exprès de l'intéressé, à moins qu'il ne soit fait exception à cette interdiction pour des motifs d'intérêt public, par décret en Conseil d'Etat pris sur proposition ou avis conforme de la Commission.

Dans le cas d'espèce, la Commission prend acte de ce que la procédure consistant à autoriser la collecte d'informations relevant de l'article 31 de la loi du 6 janvier 1978 par décret en. Conseil d'État a été retenue pour la mise en œuvre du décret du 13 juillet 2000 et estime que l'objectif poursuivi par le gouvernement, qui est d'accorder des aides financières aux orphelins dont les parents ont été victimes des persécutions antisémites intervenues durant l'Occupation, constitue un motif d'intérêt public.

Toutefois, la Commission considère que la rédaction du décret doit être modifiée afin d'encadrer aussi strictement que possible la dérogation apportée à l'article 31 de la loi du 6 janvier 1978.

En conséquence, la Commission émet un avis favorable sur le projet de décret portant application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers mis en œuvre pour l'application du décret n° *2000-657* du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites, sous réserve qu'il soit rédigé comme suit : « En application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 susvisée, et aux seules fins d'instruction des demandes présentées au titre du décret n° 2000-657 du 13 juillet 2000 instituant une mesure de réparation pour les orphelins dont les parents ont été victimes de persécutions antisémites et de versement des indemnités en capital et des rentes viagères servies en application de ce même décret, le secrétariat général du Gouvernement, la direction des statuts, des pensions et de la réin-

sertion sociale du ministère de la Défense et l'Office national des anciens combattants et victimes de guerre sont autorisés à collecter et à traiter, dans le cadre des traitements automatisés créés par le décret susvisé, les informations nécessaires pour l'accomplissement de ces finalités ». Parallèlement, il conviendrait que ce texte vise le décret portant création des deux traitements mis en oeuvre.

Délibération 01-006 du 25 janvier 2001 portant avis sur un projet de décision présenté par l'établissement public du Musée du Louvre concernant un traitement de contrôle des accès et des horaires de certains personnels par la reconnaissance du contour de la main

(Demande d'avis n° : 729309)

La Commission nationale de l'informatique et des libertés ; Saisie pour avis du projet de décision présenté par l'établissement public du Musée du Louvre ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu les articles L. 121-8 et L. 611-9 du code du travail ; Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu Monsieur Hubert Bouchet, vice président délégué, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le Musée du Louvre a déposé un dossier de demande d'avis auprès de la Commission ayant pour finalité le contrôle des heures de travail des salariés des entreprises sous-traitantes chargées d'assurer le nettoyage et la maintenance du Musée du Louvre et assurer la sécurité des œuvres d'art du musée.

Le Musée du Louvre sous-traite un certain nombre d'activités à des entreprises extérieures, les contrats de sous-traitance prévoient un certain nombre d'heures travaillées qui constituent la base d'évaluation du forfait du marché et le Musée veut contrôler la réalité des heures travaillées. La finalité initiale de ce dispositif consiste donc dans un contrôle global des heures par entreprises.

Par ailleurs compte tenu de la présence des œuvres d'arts, chacun des agents des entreprises sous-traitante doit être agréé et le Musée du Louvre demande lors de l'agrément le bulletin n° 2 du casier judiciaire. L'utilisation de la technique biométrique permet donc aussi de s'assurer que seuls les salariés agréés pénétreront dans le musée pour l'exécution du marché.

La finalité essentielle du choix d'un dispositif biométrique consiste dans la nécessité d'assurer la sécurité des biens du musée.

L'outil est composé de plusieurs bornes associées à un ordinateur qui stocke les informations par le biais d'une interface spécifique. Lorsque l'image de la main d'une personne doit être enregistrée dans le dispositif, trois mesures sont effectuées de façon à obtenir la forme de la main en trois dimensions.

La lecture de la géométrie de la main se fait en introduisant la main dans la borne, paume tournée vers le bas, de façon à ce que les doigts touchent des ergots qui permettent un positionnement correct. Lorsque la main est placée, la personne doit composer un code personnel composé de quatre chiffres et l'association du code et de la main déclenche l'ouverture de la porte et l'enregistrement des heures d'arrivée et de départ de la personne.

Le système est paramétrable de façon à autoriser un niveau de rejet général plus ou moins élevé selon la sécurité nécessaire.

Le dispositif qui est prévu pour déclencher des ouvertures de porte comporte de façon optionnelle un ordinateur qui enregistre les transactions : heures de passage associées au code de la personne, ainsi qu'une gestion des alarmes et des refus de passage.

Les informations relatives à l'identité de la personne sont conservées par le Louvre tant que le salarié fait partie de l'entreprise prestataire de service et les données relatives aux heures de passage sont conservées pendant un an sur support numérique. La durée de conservation est justifiée par l'obligation incombant aux entreprises de conserver à la disposition des inspecteurs du travail les éléments constitutifs du temps de travail des salariés pendant une année.

Dès lors, tant les informations que leur durée de conservation sont pertinentes et non excessives au regard de la finalité du traitement.

Les salariés de toutes les entreprises concernées ont été informés par note de service de l'existence de leur droit d'accès aux données les concernant et de leur droit de rectification de ces mêmes informations.

L'élément d'identification physique retenu, consistant en des mesures de la main, est difficilement susceptible d'être utilisé à des fins étrangères à la finalité recherchée par le responsable du traitement. En effet, le contour de la main ne fait pas partie des données biométriques qui laissent des traces, telles les empreintes digitales, pouvant être exploitées à des fins d'identification.

Le recours à la technique de reconnaissance du contour de la main permet de s'assurer que les données nécessaires au contrôle de l'accès ne sont ni perdues, ni falsifiées, ni échangées, que seules les personnes habilités peuvent pénétrer dans les locaux protégés et présente ainsi un degré de fiabilité. Le traitement apparaît dès lors adapté et proportionné aux objectifs poursuivis par le Musée du Louvre.

Toutefois, la Commission souhaite obtenir un bilan de l'utilisation de cette technique biométrique après douze mois d'utilisation et se prononcera à titre définitif sur le projet de décision à la lumière de ce bilan.

Au bénéfice de ces observations, la Commission émet un avis favorable au projet de décision présenté par le Musée du Louvre pour une durée d'un an.

Délibération n° 01-009 du 22 février 2001 portant avis sur le projet de décision portant création d'un fichier des enquêtes au sein du service de l'inspection de la Commission des opérations boursières

(Demande d'avis n° 726218)

La Commission nationale de l'informatique et des libertés ;

Saisie par la Commission des opérations de bourse (COB) d'une demande d'avis relative à la mise en œuvre, au sein de son service de l'inspection, d'un traitement automatisé de données nominatives dénommé « fichier des enquêtes » et ayant pour finalité la conservation et la gestion d'informations utiles à la constatation des infractions que la COB a pour mission de rechercher et plus particulièrement la tenue d'un répertoire des personnes rencontrées au cours des enquêtes effectuées par ce service ;

Vu la Convention du 28 janvier 1981 du Conseil de l'Europe 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 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le code monétaire et financier, notamment ses articles L. 621-1 à L. 621.21 et L. 642-1 à L. 642-3 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 précitée ;

Vu le projet de décision du président de la Commission des opérations de bourse ;

Après avoir entendu Monsieur Pierre Leclercq, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

La Commission des opérations de bourse (COB) a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis relative à la mise en œuvre, au sein de son service de l'inspection, d'un traitement automatisé de données nominatives dénommé « fichier des enquêtes » et ayant pour finalité la conservation et la gestion d'informations utiles à la constatation des infractions que la COB a pour mission de rechercher et plus particulièrement la tenue d'un répertoire des personnes rencontrées au cours des enquêtes effectuées par ce service.

La COB, autorité administrative indépendante régie par les dispositions des articles L. 621-1 à L. 621.21 et L. 642-1 à L. 642-3 du code monétaire et financier, est chargée de veiller à la protection de l'épargne investie dans les instruments financiers et tous autres placements donnant lieu à appel public à l'épargne, à l'information des investisseurs et au bon fonctionnement des marchés d'instruments financiers.

Aux termes de l'article L. 621-10 du code précité, elle dispose notamment, pour mener à bien sa mission, d'enquêteurs habilités qui peuvent se faire communiquer et obtenir copie de tous documents, convoquer et entendre toute personne susceptible de leur fournir des informations et accéder aux locaux à usage professionnel.

Le traitement envisagé a pour finalité de recenser des informations concernant les personnes auditionnées par le service de l'inspection de la COB et celles ayant fait l'objet, à l'issue d'une enquête, soit d'une lettre d'observation, soit de l'ouverture d'une procédure de sanction par la COB, soit de la transmission du dossier à une autre autorité, nationale ou étrangère, compétente en la matière ou au procureur de la République.

Les informations nominatives recensées dans ce traitement sont : l'identité des personnes physiques concernées (nom, prénoms, date et lieu de naissance , leurs fonctions au moment de l'enquête, l'identité de leur employeur et de a personne morale dans laquelle l'intéressé occupe, le cas échéant, une fonction de dirigeant, le lieu de commission des faits (département ou ville), les noms et numéros de l'enquête et, enfin, la suite donnée à l'enquête sous la forme d'un code (1) : classement; 2) : lettre d'observation de la COB ; 3) : ouverture d'une procédure de sanction administrative ; 4) : transmission au parquet ; 5) : au Conseil des marchés financiers ; 6) : au Conseil de discipline de la gestion financière ; 7) : à la Commission bancaire ; 8) : à la Commission de contrôle des assurances ; 9) : à la Compagnie nationale des commissaires aux comptes ; 10) : à une autorité étrangère). Ces informations apparaissent pertinentes au regard de la finalité du traitement.

Les informations nominatives traitées seront conservées dix années sur support informatique à partir du jour soit de la transmission du rapport d'enquête à un rapporteur désigné par le président de la COB, à une autorité nationale compétente ou au procureur de la République, soit de son classement.

Les décisions de classement, décisions administratives ne faisant pas grief et n'étant pas nécessairement définitives, figureront dans le fichier des enquêtes, à l'instar des autres informations concernant une enquête donnée. En conséquence, les personnes concernées pourront en avoir communication à l'occasion de l'exercice de leur droit d'accès, qui s'exercera directement à l'égard des informations figurant dans le fichier des enquêtes.

Seuls auront accès au contenu de ce fichier, en raison de leurs fonctions, les enquêteurs du service de l'inspection de la COB titulaires d'une habilitation, et ce dans le cadre strict de leurs activités professionnelles. En outre, ces personnels ne pourront interroger directement le fichier dont la création est envisagée, tâche qui sera dévolue à une seule personne. Ces possibilités d'interrogation seront limitées à trois critères : le nom de famille de la personne concernée, la raison sociale de l'entreprise concernée ou le nom donnée à l'enquête.

S'agissant des mesures de sécurité, le fichier projeté sera implanté sur un poste unique qui ne sera pas en réseau et ne sera connecté à aucun autre fichier ; son accès sera protégé par un mot de passe.

En application des dispositions de l'article 45 de la loi du 16 juillet 1992 portant adaptation au marché unique européen de la législation applicable en matière d'assurance et de crédit et de celles de l'article 68 de la loi du 2 juillet 1996 relative à la modernisation des activités financière, il est prévu que les autorités nationales en relation avec le service de l'inspection de la COB puissent être rendues destinataires des analyses, expertises et conclusions des enquêtes menées par ce service. En aucun cas ces autorités ne seront destinataires d'informations nominatives issues directement du fichier projeté

La COB peut également, aux termes de l'article L. 621 -21 du code monétaire et financier, communiquer, à leur demande et sous réserve de réciprocité, les informations qu'elle détient ou recueille aux autorités des États membres des communautés européennes exerçant des compétences analogues et tenues au même respect du secret professionnel ou à des autorités des autres États parties à l'accord sur l'espace économique européen.

En cas de transmission d'informations à des autorités étrangères, le service de l'inspection rappellera systématiquement à ses homologues les obligations de confidentialité et de secret qui s'attachent à cette communication.

Toutefois, ces différentes autorités, nationales comme étrangères, n'étant pas visées en tant que destinataires, la COB devra avant publication compléter l'article 3 du projet de décision portant création du traitement envisagé sur ce point.

La COB a souhaité faire application des dispositions du dernier alinéa de l'article 27.

La COB a également souhaité exclure, en application de l'article 26 de loi, la possibilité pour les intéressés de s'opposer à ce que des informations nominatives les concernant soient saisies et traitées dans le fichier projeté.

Prend acte de l'engagement du président de la COB d'informer les intéressés de leurs droits par une référence dans la brochure intitulée *Vos droits à l'occasion d'une enquête de la Commission des opérations de bourse.*

Émet, au bénéfice de ces observations, et sous réserve que soit modifié l'article 3 du projet d'acte réglementaire portant création du fichier des enquêtes de la COB s'agissant des destinataires des informations enregistrées dans ce traitement, un avis favorable à la création, par le projet de décision qui lui est soumis, de ce traitement.

Délibération n° 01-011 du 8 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public

La Commission nationale de l'informatique et des libertés ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et notamment son article 6 ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et notamment en son article 8 ;

Vu la loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu les articles 226-13 et 226-14 du code pénal relatifs au secret professionnel ;

Vu le code de la santé publique ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978, et notamment son article premier ;

Vu le décret n° 95-100 du 6 septembre 1995 portant code de déontologie médicale ;

Vu la délibération n° 97 -008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel ;

Après avoir entendu Monsieur Alain Vidalies en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

La Commission considère que la mise en œuvre des sites Web consacrés à la santé répond à un besoin légitime d'information du public. Toute personne consultant un tel site doit se voir garantir la délivrance d'une information de qualité mais aussi la protection de ses données personnelles. La Commission a procédé à l'évaluation de sites de santé et à plusieurs vérifications sur place afin d'apprécier l'application des règles de protection des données par les sites de santé. Elle a constaté que les dispositions de la loi du 6 janvier 1978 ne sont pas appliquées de manière satisfaisante, s'agissant notamment de l'information des internautes sur l'utilisation qui peut être faite de leurs données et sur leurs droits.

Les données de santé à caractère personnel, parce qu'elles relèvent de l'intimité de la vie privée, doivent faire l'objet d'une protection particulière, exigée tant par l'article 6 de la convention h° 108 du Conseil de l'Europe que par l'article 8 de la directive européenne du 24 octobre 1995. À cet égard la Commission réaffirme la pertinence de sa recommandation du 4 février 1997 sur le traitement des données de santé à caractère personnel : les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et à des fins de santé publique, dans les conditions définies par la loi.

Les données de santé revêtant un caractère directement ou indirectement nominatif, qu'elles aient été communiquées au site par l'internaute et/ou par un professionnel de santé, ne devraient pas pouvoir être exploitées à des fins commerciales ni transmises à quiconque à des fins commerciales ou de prospection commerciale. Le respect de ce principe devrait s'imposer aux sites Web de santé appelés à recueillir des données nominatives de santé mais aussi aux sociétés et organismes susceptibles de gérer et de conserver, pour le compte de professionnels de santé ou d'établissements de santé, des dossiers médicaux accessibles sur Internet.

Le traitement des données de connexion associées à des données nominatives telles que l'adresse e-mail ou le nom de l'internaute, si elles ne révèlent pas en tant que telles l'état de santé de l'internaute, revêtent toutefois une sensibilité particulière. En effet, si de telles données issues des consultations des pages des sites Web, étaient associées à des informations nominatives, il serait à craindre qu'elles puissent être utilisées à des fins étrangères à l'intérêt de l'usager (compagnies d'assurance, employeurs, banques...). En conséquence les internautes devraient être clairement informés des finalités poursuivies et toute exploitation nominative des données de navigation ainsi que toute cession à des tiers de telles données devraient être subordonnées au consentement exprès de la personne concernée, recueilli par le biais d'une case à cocher.

Enfin, compte tenu des risques de divulgation et d'utilisation détournée des informations inhérents au réseau Internet, la confidentialité des informations médicales nominatives appelées à circuler sur le réseau devrait être garantie par le recours systématique ci des moyens de chiffrement.

Le souci d'une meilleure application de la loi par les sites de santé conduit la Commission à recommander la mise en œuvre des mesures suivantes.

Indication de la raison sociale et du siège social du site

L'indication de la raison sociale et du siège social du site devrait apparaître clairement dès la page d'accueil ou dans une rubrique accessible dès la page d'accueil (par exemple sous le titre « Qui sommes-nous »).

En outre, l'identité de la personne désignée pour assurer le respect des règles de protection des données et en particulier de la confidentialité des données de santé devrait être précisée.

Création d'une rubrique « Informatique et Libertés/Protection des données personnelles »

Une rubrique d'information devrait être conçue de façon distincte sous un titre spécifique et être accessible dès la page d'accueil. Le texte de cette rubrique devrait être concis et rédigé clairement, afin d'être compréhensible par chacun. Le responsable du site devrait y indiquer :

1) Qu'en France et en Europe les données personnelles de santé sont protégées par la loi (article 226-13 du code pénal, loi du 6 janvier 1978, directive européenne du 24 octobre 1995).

Qu'au cours de la navigation sur le site, selon les pages visitées ou les services qui intéressent l'internaute, il pourra être amené à communiquer des informations le concernant susceptibles de révéler son état de santé.

Que les données de santé revêtant un caractère directement ou indirectement nominatif, qu'elles aient été communiquées par l'internaute et/ou par un professionnel de santé, ne font l'objet d'aucune exploitation commerciale et ne sont transmises à quiconque à des fins commerciales ou de prospection commerciale.

2) Si les données collectées auprès de l'internaute ou résultant de sa navigation sur le site sont réservées à un usage strictement interne ou non.

3) Quel usage sera fait de l'adresse e-mail et/ou des coordonnées (nom et/ou adresse) de l'internaute dans le cas où ceux-ci sont collectés.

4) Qu'en aucun cas la cession ou la mise à disposition à des tiers, à des fins commerciales, de l'adresse e-mail ou des coordonnées de l'internaute, (à l'exclusion de toutes données relatives à l'état de santé réelles ou présumé de ce dernier) ne pourra être opérée sans qu'il ait été préalablement mis en mesure de s'y opposer, par le biais d'une case à cocher.

5) Que l'internaute qui aura communiqué son adresse e-mail et/ou ses coordonnées pourra à tout moment se faire radier de tout fichier et de tout traitement auxquels ces informations ont donné lieu.

6) Si les données de connexion seront ou non exploitées sous une forme directement nominative ou non.

7) Quelles exploitations éventuelles des données de connexion sous une forme nominative sont réalisées.

Dans une telle hypothèse, il devrait être précisé à l'internaute si ces données sont ou non susceptibles d'être mises à la disposition de tiers, notamment à des fins commerciales.

Dans les deux cas, une telle exploitation des données de connexion associées à des données nominatives ne peut être réalisée qu'avec l'accord des personnes, recueilli par le biais d'une case à cocher.

8) Lorsque des « cookies » sont utilisés, les buts poursuivis par leur mise en œuvre ainsi que les conséquences de leur désactivation par l'internaute.

9) La durée de conservation des informations directement nominatives (adresse e-mail, coordonnées, données de santé, autres...) ainsi que la durée de conservation des données de connexion. Ces durées doivent être limitées et proportionnées aux finalités du traitement de telles données.

10) Les coordonnées ou l'adresse e-mail du service ou du correspondant en charge de répondre aux demandes de droit d'accès, de rectification et de suppression présentées par les internautes. Ce droit devrait pouvoir s'exercer à tout moment en ligne.

Collecte directe de données auprès de l'internaute

Toute collecte directe de données auprès de l'internaute (sous forme ou non de questionnaire) devrait être accompagnée d'une information précisant, sur le support de collecte, le caractère obligatoire ou facultatif du recueil de chaque information demandée (par exemple par le biais d'un astérisque).

Dans l'hypothèse où il est envisagé de mettre à la disposition ou de céder à des tiers à des fins commerciales des données telles que l'adresse e-mail ou les coordonnées de l'internaute, à l'exclusion de toutes données relatives à l'état de santé réel ou présumé de ce dernier, l'internaute doit être mis en mesure de pouvoir s'y opposer en ligne par le biais d'une case à cocher devant figurer sur le support de collecte.

À défaut d'une telle mention sur le support de collecte, les données seront supposées être destinées à un usage exclusivement interne.

Mesures de confidentialité et de sécurité

Des mesures de sécurité reposant notamment sur le recours à des moyens de chiffrement ainsi que sur des dispositifs de journalisation des connexions devraient être mises en place pour assurer l'intégrité et la confidentialité des données.

Le contrat passé avec un hébergeur tiers devrait comporter des clauses prévoyant les nécessaires mesures destinées à assurer la sécurité des données, ainsi que leurs seuls accès et utilisation par des personnes habilitées à en connaître.

Ces mesures doivent être portées à la connaissance de la CNIL lors de l'accomplissement des formalités préalables.

Forum de discussion

Une mention d'information devrait préciser que l'espace de discussion est destiné à permettre aux internautes d'apporter leur contribution aux thèmes de discussion proposés et que les données qui y figurent (adresse e-mail et/ou coordonnées notamment) ne peuvent être collectées ou utilisées à d'autres fins, et tout particulièrement à des fins commerciales ou de prospection.

Il est recommandé qu'un modérateur soit chargé de supprimer les contributions susceptibles d'engager la responsabilité du site ou de porter atteinte à la considération ou à l'intimité de la vie privée d'un tiers.

La possibilité de participer au forum sans avoir à s'identifier devrait être offerte à l'internaute, notamment lorsque l'espace de discussion comporte un modérateur.

Les intervenants devraient être informés de leur droit de demander à tout moment la suppression de leurs contributions en s'adressant au service en charge du droit d'accès.

Le développement des sites de santé sur Internet conduit la Commission à souhaiter que le principe de l'interdiction de toute commercialisation de données de santé directement ou indirectement nominatives soit posé par la loi, comme l'est déjà, dans le code de la santé publique, l'interdiction d'utiliser à *des* fins de prospection commerciale des données relatives aux prescriptions des médecins lorsqu'elles revêtent à leur égard un caractère directement ou indirectement nominatif.

Par ailleurs la possibilité désormais offerte par des sociétés de service d'assurer l'hébergement de dossiers de santé, accessibles par Internet, conduit la Commission, à appeler l'attention des pouvoirs publics sur la nécessité de prévoir des garanties sérieuses de nature à prévenir tout risque de divulgation ou d'utilisation indue des données et d'envisager, le cas échéant, une procédure d'agrément de tels organismes.

Délibération n° 01 -012 du 8 mars 2001 portant avis sur un projet de décision présenté par l'association pour la bonne coordination médico-chirurgicale concernant la mise en place d'un réseau ville-hôpital destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients bénéficiant d'une prise en charge médico-chirurgicale

(Demande d'avis n° 716912)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis du projet de décision présenté par l'Association pour la bonne coordination médico-chirurgicale ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu Monsieur Alain Vidalies, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

L'Association pour la bonne coordination médico-chirurgicale (ABCMC) qui a pour objet la prise en charge médico-chirurgicale de patients adultes a saisi la Commission d'une demande d'avis ayant pour finalité l'expérimentation dans le cadre d'un réseau ville-hôpital d'un dossier de santé électronique sécurisé (« coffre fort électronique ») accessible sur Internet. Participent au réseau les médecins des services de radiologie, de biophysique, de biologie et les services cliniques participant à la prise en charge

médico-chirurgicale des patients ainsi que les médecins libéraux qui le souhaitent et qui auront adhéré à cette association.

Le dossier de santé électronique sera constitué et alimenté par les médecins assurant le suivi des patients et comportera les observations, prescriptions, résultats d'examens, diagnostics et traitements mais également des radiographies, scanners, échographies, IRM.

Sur les conditions de constitution et d'accès, par les usagers, au dossier de santé électronique

La Commission prend acte de ce que l'accord exprès de l'usager sera recueilli pour autoriser la création du dossier de santé électronique et que son consentement sera effectivement requis pour autoriser l'accès de ses données à d'autres professionnels de santé. La Commission estime que le professionnel de santé devra être averti, par un message spécifique, de la nécessité de recueillir le consentement de la personne Tors de la communication à d'autres professionnels de santé de données du dossier de santé. La Commission observe que le patient pourra accéder directement par Internet à certaines parties de son dossier médical et en particulier à sa fiche signalétique qui comporte son identité, son adresse, des données d'alerte médicales, l'identité des médecins traitants et un aide-mémoire personnel que lui seul peut visualiser. Le dossier de santé comporte également une fiche de liaison retraçant certains événements médicaux dont l'accès ne lui serait reconnu qu'après accord du professionnel de santé auteur de l'information. La Commission considère à cet égard, que la possibilité désormais ouverte à chacun de pouvoir accéder en temps réel sur Internet à son dossier de santé devrait s'accompagner d'une maîtrise plus large des informations médicales appelées à figurer sur son dossier.

Elle estime que le document qui sera remis à l'usager lors de la création du dossier de santé électronique devra indiquer clairement les modalités prévues de constitution, de mise à jour et d'accès au dossier ainsi que les conséquences de l'utilisation, par les professionnels de santé dudit dossier, les conditions dans lesquelles l'usager pourra lui-même accéder directement aux informations contenues dans ce dossier et, éventuellement, les cas où il devra s'adresser à un médecin pour obtenir communication de certaines des informations contenues dans ce dossier et enfin, l'identité de la société appelée à héberger les dossiers ainsi que les engagements de confidentialité prises par celle-ci.

La Commission considère que la remise de ce document doit être préalable au recueil du consentement exprès de l'usager pour la constitution de son dossier de santé, ce consentement pouvant être retiré et/ ou modifié à tout moment.

Sur les conditions d'accès et de validation des informations par les professionnels de santé

La Commission observe que, dans le cadre de la phase expérimentale du projet, les accès des professionnels de santé seront assurés par des procédures de codes d'accès et de mots de passe attribués par le médecin désigné comme administrateur fonctionnel du réseau après que l'identité et la qualité des médecins ait été vérifiée auprès du Conseil de l'Ordre ; qu'à terme, l'identification, l'authentification ainsi que la signature électronique du professionnel de santé seront assurés par la carte de professionnel de santé.

La Commission estime que le recours à ce procédé permet d'assurer effectivement l'identification et l'authentification du professionnel de santé ; que chaque professionnel de santé participant au réseau devra en être doté dans les délais les plus rapides ; qu'à défaut, il conviendra que dans un délai de six mois à compter de la publication du décret d'application de la loi du 13 août 2000, un procédé de signature électronique soit mis en place.

La Commission estime, en outre, que la participation des professionnels de santé au réseau devra s'accompagner d'une définition précise, par voie contractuelle, des conditions de leur adhésion et de leur responsabilité respective dans la gestion sur Internet des dossiers médicaux de leurs patients.

Sur l'intervention de sociétés commerciales dans le traitement du dossier de santé sur Internet

Le projet prévoit que l'exploitation du serveur hébergeant les dossiers de santé électroniques est assuré en France par la société Accenture. La Commission estime que l'intervention de sociétés commerciales dans la gestion des systèmes d'informations de santé appelle une vigilance particulière et qu'elle doit s'entourer de garanties appropriées de nature à éviter en particulier toute utilisation des données à des fins autres que celles pour lesquelles elles ont été collectées ainsi que toute cession à des tiers. À cet égard, la Commission prend acte des dispositifs de sécurité retenus pour assurer la sécurité physique et logique des dossiers de santé. Les informations appelées à circuler sur le réseau Internet feront l'objet d'un chiffrement à 128 bits suivant le protocole SHL et le déchiffrement des données ne pourra être effectué que par les professionnels de santé disposant de droits d'accès aux données.

La Commission prend également acte de l'engagement de la société Accenture de ne pas exploiter les données à des fins commerciales et de ne pas les céder à des tiers.

Compte tenu de ses observations la CNIL émet un avis favorable pour une durée de trois ans au projet d'acte réglementaire présenté par l'Association pour la bonne coordination médico-chirurgicale concernant la mise en place, à titre expérimental, d'un réseau ville-hôpital destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients et demande à être saisie d'un bilan de fonctionnement du réseau.

Délibération n° 01-013 du 8 mars 2001 portant avis sur un projet de décision présenté par l'Association Intégrale Santé concernant la mise en place d'un réseau de soins dans la région de Lens destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients

(Demande d'avis **n°** 729637)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis du projet de décision présenté par l'Association Intégrale Santé de Lens ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu l'arrêté du 1er août 2000 portant agrément d'une action expérimentale en application de l'article L. 162-31-1 du code de la sécurité sociale ;

Après avoir entendu Monsieur Alain Vidalies, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

L'Association Intégrale Santé regroupe les professionnels de santé de Lens qui ont crée le « réseau global d'exercice du bassin de vie de Lens et sa région », réseau agrée par le Comité d'orientation des filières et des réseaux de soins tel que prévu par l'article L. 162-31-1 du code de la Sécurité sociale. Cette association a saisi la CNIL d'une demande d'avis ayant pour finalité la mise en place à titre expérimental d'un dossier de santé électronique accessible sur Internet aux patients et aux différents acteurs impliqués dans le réseau et ce pour assurer une meilleure coordination des soins entre les professionnels de santé libéraux volontaires, le centre hospitalier de Lens et la caisse primaire d'assurance maladie de Lens. La population concernée serait constituée des assurés ou ayants droit relevant du régime général résidant dans l'agglomération de Lens ainsi que dans les communes d'Avion, Méricourt, Rouvroy et Drocourt.

Le dossier de santé électronique sera constitué et alimenté par les médecins assurant le suivi des patients et comportera les observations, prescriptions, résultats d'examens, diagnostics et traitements mais également des radiographies, scanners, échographies, IRM.

Sur *les conditions de constitution et d'accès, par les usagers, au dossier de santé électronique*

La Commission prend acte de ce que l'accord exprès de l'usager sera recueilli pour autoriser la création du dossier de santé électronique et que son consentement sera effectivement requis pour autoriser l'accès de ses données à d'autres professionnels de santé. La Commission estime que le professionnel de santé devra être averti, par un message spécifique, de la nécessité de recueillir le consentement de la personne Tors de la communication à d'autres professionnels de santé de données du dossier de santé.

La Commission observe que le patient pourra accéder directement par Internet à certaines parties de son dossier médical et en particulier à sa fiche signalétique qui comporte son identité, son adresse, des données d'alerte médicales, l'identité des médecins traitants et un aide-mémoire personnel que lui seul peut visualiser. Le dossier de santé comporte également une fiche de liaison retraçant certains événements médicaux dont l'accès ne lui serait reconnu qu'après accord du professionnel de santé auteur de l'information.

La Commission considère à cet égard, que la possibilité désormais ouverte à chacun de pouvoir accéder en temps réel sur Internet à son dossier de santé devrait s'accompagner d'une maîtrise plus large des informations médicales appelées à figurer sur son dossier.

Elle estime que le document présenté sous forme de charte qui sera remis à l'usager lors de la création au dossier de santé électronique devra indiquer clairement les modalités prévues de constitution, de mise à jour et d'accès au dossier ainsi que les conséquences de l'utilisation, par les professionnels de santé dudit dossier, les conditions dans lesquelles l'usager pourra lui-même accéder directement aux informations contenues dans ce dossier et, éventuellement, les cas où il devra s'adresser à un médecin pour obtenir communication de certaines des informations contenues dans ce dossier et enfin, l'identité de la société appelée à héberger les dossiers ainsi que les engagements de confidentialité prises par celle-ci.

La Commission considère que la remise de ce document doit être préalable au recueil du consentement exprès de l'usager pour la constitution de son dossier de santé, ce consentement pouvant être retiré et/ou modifié à tout moment.

Sur les conditions d'accès et de validation des informations par les professionnels de santé

La Commission observe que, dans le cadre de la phase expérimentale du projet, les accès des professionnels de santé seront assurés par des procédures de codes d'accès et de mots de passe attribués par le médecin désigné comme administrateur fonctionnel du réseau après que l'identité et la qualité des médecins ait été vérifiée auprès du Conseil de l'Ordre ; qu'à terme, l'identification, l'authentification ainsi que la signature électronique du professionnel de santé seront assurés par la carte de professionnel de santé.

La Commission estime que le recours à ce procédé permet d'assurer effectivement l'identification et l'authentification du professionnel de santé ; que chaque professionnel de santé participant au réseau devra en être doté dans les délais les plus rapides ; qu'à défaut, il conviendra que dans un délai de six mois à compter de la publication du décret d'application de la loi du 13 août 2000, un procédé de signature électronique soit mis en place.

La Commission estime, en outre, que la participation des professionnels de santé au réseau devra s'accompagner d'une définition précise, par voie contractuelle, des conditions de leur adhésion et de leur responsabilité respective dans la gestion sur Internet des dossiers médicaux de leurs patients.

Sur l'intervention de sociétés commerciales dans le traitement du dossier de santé sur Internet

Le projet prévoit que l'exploitation du serveur hébergeant les dossiers de santé électroniques est assuré en France par la société Accenture.

La Commission estime que l'intervention de sociétés commerciales dans la gestion des systèmes d'informations de santé appelle une vigilance particulière et qu'elle doit s'entourer de garanties appropriées de nature à éviter en particulier toute utilisation des données à des fins autres que celles pour lesquelles elles ont été collectées ainsi que toute cession à des tiers.

À cet égard, la Commission prend acte des dispositifs de sécurité retenus pour assurer la sécurité physique et logique des dossiers de santé. Les informations appelées à circuler sur le réseau Internet feront l'objet d'un chiffrement à 128 bits suivant le protocole SHL et le déchiffrement des données ne pourra être effectué que par les professionnels de santé disposant de droits d'accès aux données.

La Commission prend également acte de l'engagement de la société Accenture de ne pas exploiter données à des fins commerciales et de ne pas les céder à des tiers.

Compte tenu de ses observations la CNIL émet un avis favorable pour une durée de trois ans au projet d'acte réglementaire présenté par l'Association Intégrale Santé de Lens concernant la mise en place, à titre expérimental, d'un réseau de soins dans la région de Lens destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients et demande à être saisie d'un bilan de fonctionnement du réseau.

Délibération n° 01-014 du 8 mars 2001 portant avis défavorable sur le traitement automatisé d'informations nominatives mis en œuvre par La Poste dans le cadre d'une expérimentation dite « référentiel *des* boîtes aux lettres »

(Demande d'avis n° 693603)

La Commission nationale de l'informatique et des libertés, saisie pour avis le 20 décembre 2000 par le président de La Poste d'un projet de décision portant création d'un traitement automatisé d'informations nominatives dénommé « référentiel des boîtes aux lettres » ;

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

Vu la directive n° 95/46/ CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu l'arrêté du 4 avril 1990 portant création d'un traitement automatisé d'informations nominatives dit « référentiel adresse ».

Vu la délibération de la Commission n° 86-030 du 11 mars 1986 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Poste a saisi la CNIL d'un projet de demande d'avis relatif à un traitement automatisé intitulé « référentiel des boîtes aux lettres », appelé à comporter des informations de localisation des points de distribution de courrier, associés, pour chacun d'entre eux, au nom du « foyer postal » entendu comme le nom d'une des personnes vivant dans un même domicile ;

Ce traitement est présenté comme poursuivant deux finalités : d'une part, apporter une aide aux facteurs devant distribuer le courrier par l'automatisation du classement des plis en fonction des points de distribution ; d'autre part, développer la mécanisation des opérations de tri, l'un et l'autre de ces

objectifs devant contribuer à réduire le nombre de plis ne parvenant pas à leurs destinataires.

La Poste précise que ce traitement, déjà mis en œuvre à titre expérimental dans vingt-trois établissements, devrait être développé sur treize sites supplémentaires en 2001 et dans d'autres zones géographiques l'année suivante.

La Poste, qui envisage d'informer les intéressés par la distribution d'un pli d'information, se réserve la possibilité, en cas d'absence de réponse, de relever directement le nom des personnes sur les boîtes aux lettres. Elle exclut, en application du 2e alinéa de l'article 26 de la loi du 6 janvier 1978, l'exercice du droit d'opposition à l'égard du traitement.

Le schéma d'ensemble tel qu'il résulte de la demande d'avis sur laquelle la Commission doit se prononcer appelle des réserves tant en ce qui concerne la constitution d'un fichier national nominatif que les modalités prévues pour recueillir le nom des personnes et les informer de l'existence du traitement. Aussi, sans contester la légitimité des objectifs poursuivis par La Poste, ce traitement national tel qu'il est présenté ne saurait-il recueillir, en l'état, un avis favorable.

Au bénéfice de ces observations, la Commission émet, en l'état du dossier, un avis défavorable au projet d'acte réglementaire relatif au traitement dénommé « référentiel des boîtes aux lettres ».

Délibération n° 01-016 du 20 mars 2001 portant avis sur l'avant-projet de loi présenté par l'INSEE concernant la réforme du recensement de la population

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis, par l'INSEE, conformément aux dispositions de l'article 20 du décret n° 78-774 du 17 juillet 1978, de l'avant-projet de loi relatif au recensement de la population ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe sur 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 ensemble le décret 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée et notamment son article 20 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu l'avis du Conseil d'État en date du 2 juillet 1998 ;

Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :

La CNIL, dans son 20e rapport d'activité (1999), a pris acte du projet de l'INSEE de définir une nouvelle procédure de recensement de la population. Cette procédure rénovée de recensement trouve sa justification dans les lourdeurs de mise en œuvre et le coût d'un recensement classique mais aussi dans les réticences nouvelles exprimées par les personnes à l'égard du recensement de 1999.

Le nouveau dispositif de recensement conçu par l'INSEE consistera à opérer par la voie d'un recensement classique dans des communes comportant une population inférieure à un certain seuil de population (à l'heure actuelle 10 000 habitants) mais selon un principe de rotation annuelle (une commune sur cinq étant recensée chaque année) et par voie de sondage portant sur 8 % de la population totale d'une commune dans les autres communes. Chaque année, l'INSEE procéderait à l'extrapolation des résultats obtenus d'une commune à l'autre ou d'un quartier de ville à l'ensemble de la ville grâce à un outil de référence sur la structure des populations par commune ou par quartier contigu d'environ 2 000 habitants.

Pour ce faire, et afin d'apprécier les évolutions intervenues et de les appliquer aux données collectées sur le terrain, l'INSEE envisage de se faire communiquer, notamment par les caisses d'assurance maladie, pour chaque bénéficiaire, son sexe, son année de naissance et son adresse. Ainsi, serait constitué un fichier, dépourvu de caractère directement nominatif et qui permettrait, pour chaque quartier de 2 000 habitants, de disposer de la structure de population y vivant en nombre, âge et sexe. Ce fichier à usage purement interne serait l'outil d'extrapolation des résultats.

La CNIL estime que cette nouvelle procédure peut être de nature à renforcer la confidentialité des données collectées. En effet, une collecte répartie sur cinq ans et concernant des petits volumes limiterait à quelques mois la conservation par l'INSEE des données sous leur forme nominative.

La Commission a fait part à l'INSEE, par courrier du 28 décembre 1999, que le principe de finalité des fichiers administratifs susceptibles d'être utilisés à de telles fins et l'ampleur de l'opération envisagée devrait conduire à ce que la transmission à l'INSEE de données issues de fichiers administratifs nécessaire à l'extrapolation des résultats soit posée par la loi et que les données ainsi communiquées soient agrégées par l'INSEE à un niveau géographique de nature à éviter toute réidentification des personnes.

Dans le cadre de l'avant-projet de loi portant diverses dispositions d'ordre économique et financière (DDOEF) deux articles sont soumis pour avis à la Commission : le premier porte sur la réforme du recensement de la population et le second concerne les dispositions transitoires et d'application relatives à ce dernier.

L'article 16 — I du projet de loi réaffirme la responsabilité de l'État en matière de recensement. Son article 16 — II organise la collaboration entre l'État, l'INSEE, les communes et les établissements publics de coopération intercommunale.

L'article 16 — II dernier alinéa dispose que les données recueillies lors du recensement sont régies par les dispositions de la loi du 7 juin 1951. Le souci de souligner que lés données en cause sont confidentielles et protégées devraient conduire à viser également la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

À l''article 16 — III, il est prévu que l'INSEE est chargé de la collecte des données, de l'exploitation et de la diffusion des résultats et que les communes ou leurs groupements préparent et réalisent les enquêtes du recensement.

L'article 16 — V organise les modalités de collecte des données du recensement ainsi que l'exploitation de données non nominatives issues de fichiers administratifs pour l'extrapolation des résultats.

Un souci de plus grande clarté et de plus grande précision devrait conduire à indiquer dès le premier alinéa de ce texte que les informations issues de fichiers administratifs sont des données démographiques non nominatives et, au deuxième alinéa, que les données ainsi transmises par les régimes obligatoires d'assurance maladie devront être agrégées à l'issue de chaque cycle quinquennal du recensement afin d'éviter toute réidentification des personnes.

Émet un avis favorable aux dispositions de l'avant-projet de loi qui lui est soumis en proposant que :

— L'article 16 — II dernier alinéa soit complété de la façon suivante « ainsi que par celles de la loi du 6 janvier 1978 relative à l'informatique, aux fi chiers et aux libertés ».

— L'article 16 — V soit rédigé comme suit : « Pour établir les chiffres de po pulation, l'institut national de la statistique et des études économiques utilise les informations collectées dans chaque commune par des enquêtes de re censement exhaustives ou par sondage, ainsi que des données démographi ques non nominatives issues de fichiers administratifs ou de répertoires immobiliers, que l'institut est habilité à collecter à des fins exclusivement sta tistiques.

À cette fin, les autorités gestionnaires des fichiers des organismes servant les prestations de base des régimes obligatoires d'assurance maladie transmettent à l'institut national de la statistique et des études économiques les informations non nominatives nécessaires, qu'il appartiendra à l'INSEE, à l'issue de chaque cycle quinquennal de recensement, d'agréger à un niveau géographique de nature à éviter toute réidentification des personnes ».

Délibération n° 01-017 du 3 avril 2001 portant avis favorable sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives issues de la base image « adresse de logement » créée lors du recensement général de la population 1999

(Demande d'avis **n°** 715626)

La Commission nationale de l'informatique et des libertés ; Saisie par l'INSEE d'une demande d'avis portant création d'un traitement automatisé d'informations nominatives relatif à l'exploitation de la base — image « adresse de logement » issue du recensement général de la population de 1999 ;

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

Vu la directive n° 95/46/CE du Parlement européen et du Conseil de l'Europe du 24 octobre 1995 relative à la protection des personnes physiques à

l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu la loi n°51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu l'arrêté du 22 mai 1998 portant création d'un traitement automatisé réalisé à l'occasion du recensement général de la population de 1999 ;

Vu l'arrêté du 29 juillet 1998 portant création d'un traitement automatisé par lecture optique des bulletins du recensement général de la population de 1999 ;

Vu l'arrêté du 26 février 2001 modifiant l'arrêté du 29 juillet 1998 susvisé ; Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'INSEE a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis concernant la mise en œuvre d'un traitement automatisé pour l'exploitation de la base — image « adresse de logement » (BAL), définie par l'arrêté du 29 juillet 1998, modifié susvisé, qui doit permettre la constitution de l'échantillon maître des logements à partir duquel sont réalisées les enquêtes statistiques auprès des ménages.

Le traitement considéré a pour objet la fourniture et l'impression des fiches adresses à partir des données figurant dans la « base adresse de logement » depuis le recensement général de la population de 1999 : l'adresse du logement recensé ainsi que le nom et prénom de son occupant lors du recensement.

Les fiches adresses sont remises aux enquêteurs en charge de la collecte pour leur permettre de déterminer précisément chaque logement. L'INSEE est seul destinataire des informations individuelles enregistrées. Le droit d'accès et de rectification prévu par l'article 34 de la loi du 6 janvier 1978 s'exerce auprès de la direction générale de l'INSEE.

Au bénéfice de ces observations, la Commission émet un avis favorable au projet d'arrêté qui lui est soumis.

Délibération n° 01-018 du 3 mai 2001 portant avis sur le projet de loi sur la société de l'information

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le garde des Sceaux et le secrétaire d'État à l'industrie, le 30 mars 2001, du projet de loi sur la société de l'information.

Vu la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales du 4 novembre 1950 ;

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

Vu la directive européenne 95/46 du 24 octobre 1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données ;
Vu la directive européenne n° 97/66 du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret d'application du 17 juillet 1978 ;
Après avoir entendu M. Michel Gentot, en son rapport et M. Michel Capcarrère, commissaire-adjoint du Gouvernement, en ses observations,

Émet l'avis suivant :

Le projet de loi sur la société de l'information aborde plusieurs sujets concernant Internet qui correspondent aux débats de fond que le développement du réseau suscite depuis plusieurs années dans l'ensemble des pays développés.
La CNIL se réjouit que ces débats puissent être tranchés, grâce à cette initiative législative destinée à adapter les règles de notre droit à la société de l'information, par le Parlement.
Elle rappelle que l'un des premiers débats qu'Internet a provoqués tenait à l'interrogation sur la portée ou l'efficacité de l'application d'une législation nationale à un réseau international. Aussi, souhaite-t-elle souligner que, dans le domaine de compétence qui est le sien, deux directives européennes (la directive du 24 octobre 1995 sur la protection des données personnelles et la libre circulation de ces données et la directive du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications) ont établi un socle de principes communs à l'ensemble des États membres de l'Union européenne, applicables à Internet. Plusieurs pays tiers se sont d'ailleurs, depuis lors, largement inspiré de ces principes, soit en adoptant des dispositions législatives destinées à assurer la protection des données personnelles, soit en développant des mécanismes d'auto-régulation poursuivant la même fin, lorsque le recours à de tels moyens d'agir correspondait davantage à leur manière de faire.
Ainsi, la protection des données personnelles et de la vie privée, qui faisait encore figure d'exception au moment de l'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, est devenue la règle commune en Europe. En outre, les préoccupations que l'usage grand public ou commercial du réseau ont par ailleurs suscitées, à peu près dans les mêmes termes partout dans le monde, ont fait d'Internet un puissant vecteur de transmission de la culture européenne de protection des données personnelles. Aussi la CNIL est-elle très attentive aux choix auxquels le projet de loi procède et qui auront, à n'en pas douter, un écho particulier compte tenu de l'influence française en ce domaine.
La Commission croit à cet égard devoir souligner que sous des abords qui peuvent paraître techniques, plusieurs dispositions de ce projet touchent à des sujets qui excèdent très largement les spécificités de la technologie et qui concernent l'ensemble de nos concitoyens.
Ainsi, en est-il tout particulièrement pour l'usage, policier ou commercial, qui peut être fait de données personnelles qui relèvent par nature de notre vie privée et qui sont traditionnellement protégées par le secret de nos correspondances, le secret des choix audiovisuels ou l'inviolabilité de notre do-

micile. Il en est de même pour la diffusion d'une information personnelle sur le réseau international qui concerne non seulement les internautes mais toute personne dont le nom figure sur le net.

En effet, les protocoles de communication utilisés par Internet produisent des « traces » sur notre comportement ou nos habitudes qui sont détenues par des tiers, intermédiaires techniques, tels que les opérateurs de communication, les fournisseurs d'accès et les hébergeurs de sites. Le volume des fichiers ainsi constitués et les possibilités d'exploitation des informations qu'ils comportent sont sans précédent. Aussi la question de l'utilisation qui peut être faite de telles données est-elle d'abord un débat sur la liberté dans une société numérique. Ce débat met naturellement en jeu, voire en conflit, non seulement les nécessités d'ordre public et le respect de la vie privée mais aussi la liberté du commerce et de l'industrie, ses exigences et les limites qu'imposent les capacités inédites de « ciblage », de « profilage » et de « pistage ». La capacité de diffusion des informations sur le réseau est également sans précédent. On ne peut que se réjouir de l'élargissement considérable du périmètre de la liberté d'information et de l'accès aux savoirs qui en résulte. Cependant la technologie n'est pas neutre : il n'y a pas de commune mesure entre l'affichage d'un document à la porte d'un tribunal ou d'une mairie et sa diffusion sur Internet. Avec Internet, toute information diffusée en clair devient accessible depuis quelque endroit du monde que ce soit, sans que la profusion des informations disponibles ne constitue même une limite puisque les moteurs de recherche permettent de la retrouver dans l'instant. Cette possibilité technique de diffuser, dupliquer, récupérer, à l'échelle du monde, toute information disponible sur le réseau renouvelle sans doute les termes du débat sur la portée des mesures de publicité qui doivent entourer certaines informations lorsque ces dernières revêtent un caractère nominatif. C'est la raison pour laquelle, au-delà de l'avis que le Gouvernement a, en particulier, demandé à la Commission sur les dispositions du projet relatives à la publicité non sollicitée et à la conservation des données de connexion, la CNIL fera part de ses réflexions sur les dispositions du titre I^{er} du projet relatives à l'accès à l'information.

Possibilités nouvelles d'exploitation des traces informatiques sur nos activités, possibilités sans précédent de diffusion de l'information à l'échelle mondiale : dans ces deux cas, la Commission estime que la recherche de l'intérêt général devrait s'inspirer d'une exigence de retenue. Les possibilités d'intrusion de la vie privée n'étant, désormais, nullement limitées par la technologie qui, bien au contraire, les facilite à un degré jusqu'alors jamais atteint, cette exigence pourrait clairement signifier que les autorités de l'Etat mais aussi les professionnels concernés ne s'autoriseront pas à faire tout ce que permet la technologie. Loin de toute « diabolisation » d'Internet, cette retenue devrait être perçue comme le prolongement naturel du principe de proportionnalité.

Dans cet esprit, la Commission se félicite que le principe de la liberté d'utilisation des moyens de cryptologie, y compris lorsque ces derniers recouvrent une fonction de confidentialité, soit consacré par la future loi, une telle mesure étant incontestablement décisive pour assurer la confiance. En conséquence, les observations de la Commission porteront successivement sur les problèmes liés à la conservation des données de connexion, la publicité par la voie électronique, l'accès aux données publiques et l'accès aux archives publiques.

Conservation des données de connexion (articles 17, 18 et 19 du projet de loi)

Le dispositif prévu

Le titre II « De la liberté de communication en ligne » comporte un chapitre III, intitulé « L'effacement des données relatives aux communications », relatif à ce que l'on nomme communément, mais sous un vocable à coloration technique qui pourrait en dissimuler l'importance, les données de connexion, c'est-à-dire les informations qui sont produites ou nécessitées par la technologie, qu'il s'agisse de nos communications téléphoniques ou de nos connexions au réseau Internet.

Les informations relatives à l'usage que l'on fait du téléphone ou d'Internet sont de celles qui touchent le plus intimement à notre vie privée : les personnes que l'on appelle, quand, d'où (avec le téléphone mobile), notre navigation sur Internet, les services que nous utilisons et les sites que nous consultons, l'heure exacte de nos communications ou de nos connexions, leur durée.

Cette matière est d'ailleurs si intimement liée à notre vie privée que les États membres de l'Union européenne ont estimé, au moment de l'ouverture à la concurrence du marché des télécommunications, qu'elle devait faire l'objet d'une réglementation spécifique et harmonisée. Tel est l'objet de la directive 97/66 du 15 décembre 1997 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications » que le projet de loi transpose dans notre ordre interne.

Le projet, qui vise les données de connexion dont disposent les opérateurs de téléphonie mais aussi les fournisseurs d'accès à Internet[1], pose le principe d'un effacement ou d'une anonymisation de « toute donnée technique relative à une communication lorsque celle-ci est achevée », transposant ainsi l'article 6 de la directive 97/66. Deux exceptions sont cependant ménagées pour prévoir, d'une part, que certaines données nécessaires à la facturation ou au paiement de prestations pourront être conservés jusqu'à la **fin de la période au cours de laquelle la facture peut être légalement** contestée, d'autre part et surtout, que certaines données pourront être conservées pendant une durée maximale d'un an, « pour les besoins de la recherche et de la poursuite des infractions pénales et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire de ces données ».

Le projet précise que les données qui seront conservées à de telles fins ainsi que, dans la limite prévue par la loi, leur durée de conservation seront précisées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés, qu'en aucun cas ces données ne pourront porter sur le contenu des correspondances échangées ou des informations consultées, enfin que la conservation et le traitement de ces données devront s'effectuer dans le respect des dispositions de la loi du 6 janvier 1978.

Le dispositif tel qu'il est arrêté par le projet de loi appelle plusieurs observations.

[1] Sont donc visés par ce texte les personnes physiques ou morales exploitant un réseau de télécommunications ouvert au public ou fournissant au public un service de télécommunication c'est-à-dire fournissant toute prestation incluant la transmission ou l'acheminement des signaux ou une combinaison de ces fonctions par des procédés de télécommunication.

Observation générale

En évoquant, dans un même article, les données dont la conservation est justifiée par les nécessités de la facturation — ces données étant alors accessibles à la police judiciaire selon le droit commun — et celles dont la conservation, sans utilité pour l'internaute ou l'opérateur de télécommunication, sera prescrite par la loi à des fins exclusivement policières — c'est-à-dire, pris ensemble, le droit commun et l'exception — la présentation retenue par le projet de loi a pour effet d'estomper le caractère inédit du dispositif retenu. Cet effet ne peut qu'être renforcé par l'apparent parallélisme qui est établi entre les modalités de conservation des données dans les deux hypothèses, pourtant bien distinctes : référence, dans les deux cas, à une durée de conservation d'un an[1], renvoi, dans les deux cas, à un décret en Conseil d'État pris après avis de la CNIL, référence commune aux dispositions de la loi du 6 janvier 1978.

Une telle présentation ne doit pas dissimuler les termes du débat important et légitime qui va être tranché par le législateur et qui concerne l'éventuelle utilisation par les services de police judiciaire des données liées à nos communications. L'enjeu est incontestablement d'importance à un moment où les pouvoirs publics souhaitent établir un cadre juridique suscitant la confiance pour l'entrée de la France dans la société de l'information.

Si, selon une certaine approche, les potentialités d'Internet (rapidité des communications et volatilité des informations) nécessitent la mise en place de mesures particulières propres à éviter le développement par le réseau de certaines formes de délinquance ou d'atteintes aux droits des tiers, une autre approche consiste à soutenir qu'une technologie de communication et d'information ne doit pas déroger aux principes fondamentaux de l'Etat de droit qui méritent sans doute d'être adaptés aux spécificités d'Internet mais qui ne sauraient être considérés comme caducs par le seul effet de la nouveauté technologique.

Les fermes de ce débat ne sont pas nouveaux, ni inédits en matière de nouvelles technologies. Ce fût d'ailleurs une des intuitions des législations de protection des données personnelles et de la vie privée, au premier rang desquelles figure la loi française du 6 janvier 1978 et la Convention du 18 janvier 1981 du Conseil de l'Europe pour la protection des données personnelles, que d'avoir prévu que l'informatisation de nos sociétés allait permettre la collecte, le stockage, la conservation et le traitement de données de plus en plus nombreuses sur nos comportements les plus intimes (l'usage d'une carte bancaire, la nature et le montant de nos achats, le lieu où l'on se trouve à tel moment, l'heure d'une connexion, le lieu d'où l'on passe un appel depuis un mobile, le passage à tel péage d'autoroute, etc.). Les nouvelles technologies contribuent à créer de nouveaux gisements de données qui constituent, pour la police, autant d'éléments de preuves aisément accessibles, lui offrant ainsi des possibilités d'investigation sans précédent.

Aussi, ayant pressenti que les capacités de stockage et de traitement de l'information pourraient se développer quasiment sans connaître de limites techniques — ce qui est précisément advenu — le législateur a-t-il souhaité définir, dès les premiers balbutiements de la société numérique, des garan-

[1] Ar icle L. 32-3-3 nouveau du code des postes et télécommunications, § II pour les données conservées à des fins de police, article L. 32-3-3 nouveau, § III et article L. 32-3-5 nouveau pour les données de facturation.

ties destinées à prévenir toute, rupture de l'équilibre entre les droits du citoyen et les prérogatives de l'Etat.

En subordonnant le traitement d'informations nominatives au principe de finalité (quelles données collectées et traitées et à quelles fins ?), en limitant la durée de conservation de ces données à ce que justifie la finalité des traitements en cause, en exigeant que les données conservées soient « pertinentes » et non « excessives » au regard de la finalité de la collecte et en imposant des mesures générales d'information des citoyens sur ces différents points, les lois de protection des données personnelles et de la vie privée ont décliné, à l'aube de la société de l'information, les principes fondamentaux de proportionnalité et de retenue qui avaient précédemment et successivement conduit l'Etat à s'interdire d'opérer des perquisitions de nuit au domicile d'un particulier, de saisir des objets ou des effets lui appartenant en enquête préliminaire sans son consentement exprès ou encore de le placer sous écoute téléphonique hors un cadre juridique rigoureux et dans certaines circonstances d'une gravité particulière dont l'appréciation est soumise au contrôle d'une autorité indépendante (l'autorité judiciaire pour les écoutes judiciaires, une autorité administrative indépendante pour les interceptions de sécurité).

Ces principes de protection des données personnelles n'ont nullement eu pour effet de priver la police de moyens d'action dans la mesure où, tout au contraire, ces derniers se sont développés, quasi mécaniquement, au fur et à mesure de l'informatisation de nos sociétés. C'est précisément la raison pour laquelle les législations de protection des données personnelles et de la vie privée ont posé le principe suivant : tant que des données personnelles sont conservées dans un traitement ou un fichier, elles demeurent accessibles à l'autorité judiciaire et à la police judiciaire. En revanche, sauf exception proportionnée et justifiée, des données à caractère personnel ne peuvent être conservées au-delà de ce que justifie la finalité de leur collecte ou de leur traitement initial.

Le projet de loi dérogeant à ces principes, le dispositif retenu mériterait d'être apprécié dans la plus grande clarté compte tenu des intérêts en cause.

Observations sur la conservation des données nécessaires à la facturation

S'agissant des opérateurs de téléphonie (fixe ou mobile), les données générées par nos communications (qui on appelle ? quand ? pendant combien de temps ? où ? d'où ?) sont fondamentalement liées à la facturation qui est d'ailleurs très largement déterminée par elles. Ces données sont évidemment particulièrement sensibles, mais nul ne met en cause la légitimité de leur conservation aussi longtemps que la facture peut être contestée. Sans doute la téléphonie mobile a-t-elle apporté une information supplémentaire par rapport aux informations « plus classiques » liées à la téléphonie fixe : notre localisation lorsque nous passons ou recevons un appel depuis un portable.

S'agissant de ceux des fournisseurs d'accès à Internet dont la tarification du service est liée à un forfait, les données dont la conservation est justifiée par une nécessité de facturation sont plus limitées dans la mesure où le tarif des connexions à Internet est toujours celui d'une communication locale, quels que soient la distance du serveur auquel l'abonné se connecte, la nature du site Web consulté ou l'identité du destinataire d'un message électronique.

La CNIL a déjà appelé de ses vœux[1] une harmonisation de la durée de conservation de telles données. En effet, jusqu'à présent seul l'opérateur historique était tenu, en conséquence des dispositions de l'article L. 126 du code des postes et télécommunications, de ne les conserver que pendant une durée d'un an, les règles de droit commun en matière de prescription des créances civiles autorisant les opérateurs entrants à conserver ces informations pendant le délai ordinaire de prescription, soit cinq ans, durée qui pouvait, à tous égards et compte tenu en particulier de la sensibilité des informations en cause, paraître tout à la fois excessive et susceptible de provoquer des atteintes injustifiées à la vie privée des personnes. Aussi, la CNIL ne peut-elle qu'être favorable à ce que le projet de loi consacre le principe de finalité, principe cardinal de la protection des données personnelles et de la vie privée, en prévoyant que les opérateurs ne pourront conserver les données en cause pour les besoins de la facturation et du paiement des prestations que jusqu'à l'expiration de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement et en fixant, pour tous les opérateurs, ce délai à un an. Il résultera d'un tel dispositif d'harmonisation un raccourcissement des durées de conservation actuellement pratiquées par certains opérateurs.

S'agissant d'une éventuelle utilisation de ces données par les opérateurs souhaitant commercialiser leurs propres produits et services, la Commission prend également note avec satisfaction qu'un traitement de ces données à de telles fins ne pourra être entrepris qu'avec le consentement exprès des personnes. Cette disposition, que commande la transposition de l'article 6 de la directive 97/66 du 15 décembre 1997, renforcera les garanties jusqu'alors offertes aux usagers, le droit actuel ne distinguant pas entre ces données et des données plus « classiques » telles qu'un nom ou une adresse. En revanche, le texte proposé laisse entier le problème de savoir si un tel consentement, une fois acquis, autoriserait ou non l'opérateur à conserver les données de facturation au-delà de la durée d'un an. Ce point mériterait incontestablement d'être éclairci.

De même, la CNIL prend note avec satisfaction qu'en aucun cas de telles données ne pourront être utilisées pour le compte de tiers et qu'enfin la conservation et le traitement de ces données seront soumis aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La Commission s'interroge toutefois sur la rédaction proposée pour l'article L. 32-3-3 nouveau § III du code des postes et télécommunications (article 17 du projet) qui évoque l'hypothèse d'une transmission de ces données de facturation à des tiers. Outre l'apparente contradiction entre une telle hypothèse et les garanties ci-dessus rappelées, une telle précision pourrait paraître sans réelle portée dans la mesure où la référence faite à la loi du 6 janvier 1978 suffit à autoriser une telle transmission dès lors qu'elle serait justifiée par la finalité de facturation ou de recouvrement. En définitive, le principe d'une conservation des seules données nécessaires à la facturation, la fixation de la durée de conservation de ces données à un an, quel que soit l'opérateur, ainsi que le renvoi à un décret en Conseil d'Etat pris

[1] Dans une délibération du 27 janvier 2000 portant avis sur un ayant projet de loi présenté par le secrétariat d'État à l'Industrie portant diverses dispositions d'harmonisation communautaire, 20e rapport d'activité pour 1999, p. 113 *sqq.*

après avis de la CNIL pour déterminer celles des données qui pourront être conservées à ce titre reçoivent l'approbation de la Commission.

Observations sur la conservation des données de connexion sans lien avec la facturation

— L'enjeu

Il convient d'emblée de relever qu'en faisant obligation aux opérateurs de télécommunications de conserver des données de connexion dépourvues d'utilité pour la facturation, le projet de loi ne poursuit pas un objectif d'ordre public qui serait justifié par la nécessité d'identifier les auteurs de contenus illégaux ou attentatoires aux droits des tiers (sites pédophiles, négationistes, racistes, diffamatoires et autres). En effet, la loi du 1er août 2000 a déjà établi à la charge des hébergeurs de sites mais aussi des fournisseurs d'accès — visés ensemble par l'article 43-9 nouveau de la loi du 30 septembre 1986 — une obligation générale de « détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu », dans des conditions et pour une durée qui doivent être préci sées par un décret en Conseil d'État pris après avis de la CNIL, les données ainsi conservées pouvant être requises par l'autorité judiciaire.

Le projet de loi sur la société de l'information est de portée beaucoup plus large puisqu'il concerne tous les internautes qui échangent des mails ou naviguent sur le Web, même s'ils ne créent aucun contenu accessible au public.

Certes, le projet précise que les données ainsi conservées « ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit ». Mais cette rédaction, qui se borne à un constat exclusivement technique, si elle n'est pas inexacte, pourrait cependant donner à penser que de telles données sont anodines. Or, elles ne le sont nullement dans la mesure où, comme le précise le projet par ailleurs, elles portent notamment « sur l'identification des personnes utilisatrices des services fournis par l'opérateur de télécommunication ».

Concrètement, il s'agit de faire obligation aux fournisseurs d'accès de conserver ce que l'on nomme les « adresses IP » des ordinateurs connectés aux services accessibles par Internet, adresses qui constituent l'équivalent d'un numéro minéralogique que le fournisseur d'accès attribue à l'ordinateur utilisé par l'abonné, soit de manière permanente, soit à chacune de ses connexions. La conservation de cette adresse IP permet d'identifier tout ordinateur connecté au réseau (et donc la personne physique titulaire de la ligne) et ses heures de connexion. Certes, à elle seule, la conservation de ces informations ne permet pas d'identifier l'activité de l'internaute. Mais si le projet de loi prescrit la conservation de telles données, c'est précisément pour associer à un comportement sur Internet une identité précise. La technologie d'Internet (c'est-à-dire le protocole de communication entre ordinateurs distants) permet déjà à certains robots de récupérer l'ensemble des adresses IP des ordinateurs connectés la conservation dés données de connexion par les fournisseurs d'accès permettra d'identifier individuellement leurs utilisateurs ou tout au moins la personne physique titulaire de la ligne. De même, le rapprochement des données devant être conservées par les fournisseurs d'accès avec celles dont la loi du 1er août 2000 a prescrit la conservation aux hébergeurs de sites, permettrait d'identifier, non pas seulement les per-

sonnes ayant rendu un contenu accessible sur Internet, mais beaucoup plus généralement les internautes s'étant bornés à consulter tel ou tel site.

Ces quelques précisions techniques donnent la mesure de ce qui est en cause dans le projet de loi : l'absolue et inédite transparence de notre activité d'internaute lorsque pourtant nous nous abstenons de mettre un contenu à la disposition du public via le réseau.

— Les termes du débat

Nul ne paraît contester la nécessité de prévoir des mesures de précaution afin de lutter contre certaines formes de délinquance ou de criminalité sur le réseau, tout particulièrement en matière d'intrusion ou de propagation de virus informatique. Ce souci d'intérêt public nécessite, à n'en pas douter, la conservation par les fournisseurs d'accès des données de connexion. Mais c'est la portée des mesures à prévoir à cette fin et les garanties qui doivent les entourer qui font légitimement débat depuis plusieurs années entre les acteurs de la société de l'information et les pouvoirs publics dans l'ensemble des pays développés.

Compte tenu du caractère dérogatoire aux principes généraux de protection des données personnelles et de la vie privée et, de manière plus générale, des atteintes possibles au respect de la vie privée et des libertés individuelles qu'emporte la conservation à des fins exclusivement policières de données dépourvues d'utilité technique, une fois la connexion établie entre un internaute et son interlocuteur (qu'il s'agisse de la personne physique avec laquelle l'internaute communique par courrier électronique ou d'un serveur distant, support d'un site public d'information), la sagesse et le principe de proportionnalité que commande tout particulièrement l'article 6 de la Convention de sauvegarde des Droits de l'homme et des libertés fondamentales devraient présider au débat public que le projet de loi ne manquera pas de susciter.

Les intérêts en cause sont nombreux et de nature diverse.

S'agissant des impératifs de sécurité publique, ne sont pas en cause la prévention et la recherche des contenus illégaux accessibles au public (le dispositif légal institué par la loi du 1er août 2000 y répond déjà), mais celles des actes de délinquance que la communication par le réseau pourrait faciliter ou permettre.

Il est déjà possible aux autorités de l'État, dans les conditions prévues par la loi du 1er août 1991 relative au secret des correspondances émises par la voie des télécommunications, de procéder à des interceptions de communications sur Internet, comme elles peuvent le faire pour les communications téléphoniques, ce qui résulte d'ailleurs clairement de l'article 52 du projet de loi. De telles interceptions, placées sous le contrôle du juge ou d'une autorité indépendante, permettent déjà d'identifier les comportements délictuels ou criminels.

Le projet de loi n'a donc pas pour objet de rechercher un moyen de substitution à une technique qui ne serait pas applicable à Internet — l'interception est possible sur Internet— mais à étendre les possibilités dont devraient disposer les autorités publiques, en ajoutant aux moyens traditionnels dont elles disposent déjà (les interceptions de communication), des moyens nouveaux que la technologie et les protocoles de communication permettent de mettre en œuvre (le rapprochement et l'analyse des données de connexion).

S'il a pu être regretté par les autorités policières, dans tous les pays du monde, que certains fournisseurs d'accès ne conservent que durant quelques jours les données de connexion de leurs usagers, une telle situation ne doit pas faire perdre de vue le fait que la plupart des fournisseurs d'accès, en tout cas les plus importants, conservent, à des fins de sécurité informatique interne, les données de connexion de leurs abonnés pendant une durée de l'ordre de trois mois, ces données étant alors accessibles aux forces de police, dans le cadre des enquêtes judiciaires qu'elles diligentent. Imposer une obligation de conservation des données de connexion pendant un an, au motif que, jusqu'à présent et dans le silence de la loi, certains fournisseurs d'accès ne conservaient ces données que durant quelques jours pourrait paraître, sur le terrain des libertés individuelles et publiques, manquer de mesure.

Il convient de mettre en regard des impératifs d'intérêt public, qui méritent donc d'être nuancés, **la liberté personnelle** : celle de consulter un site Internet sans avoir le sentiment d'être sous surveillance, celle de pouvoir adresser un message électronique, comme on adresse un courrier postal ou un appel téléphonique, non pas avec un sentiment particulier de liberté, tant celle-ci nous paraît acquise, mais sans calcul ni préoccupation. Le développement du minitel en France a suscité, en termes de libertés personnelles, des débats de même nature que ceux qui sont aujourd'hui abordés, s'agissant d'Internet. Ne convenait-il pas de se prémunir contre certains des usages « inconvenants » de la télématique, de veiller au respect de l'ordre public et d'une certaine civilité par les kiosques ? Le choix a pourtant été fait de ne pas lier la facturation à la nature des services offerts et de renoncer à installer une « mémoire vive »[1] dans les terminaux de sorte que la nature des services consultés par les usagers ne soit ni conservée, ni traitée. Et nul n'avance qu'en procédant ainsi l'Etat se serait désarmé face à certaines formes de délinquance. Il s'agissait, à l'heure d'une technologie jusqu'alors inédite, de s'en tenir aux principes fondamentaux de protection de la vie privée des personnes qui président également à l'accès aux services de communication audiovisuelle : en cette matière, le secret de ses choix, dans une société de libertés, devrait demeurer la règle et les exceptions très rigoureusement pesées.

Le dernier intérêt en cause, qui ne se situe pas sur le terrain des libertés mais qui mérite sans doute d'être évoqué, est celui **des fournisseurs d'accès** eux-mêmes, acteurs sans lesquels les connexions à Internet ne seraient pas possibles. Sans doute les contraintes d'une catégorie de professionnels ne sauraient-elles dicter ce que commande l'intérêt général. Cependant, c'est sur eux que pèsera, techniquement et financièrement, l'obligation de conserver pendant de longues durées les données de connexion. Les estimations les plus sérieuses évaluent le nombre de pages Web consultées par jour, en France, à 4 ou 5 milliards. S'agissant des messages électroniques, l'Association des fournisseurs d'accès précise que les abonnés des professionnels qu'elle fédère auraient envoyé, pour la seule journée du 3 janvier 2001, 3 600 000 messages. De tels volumes donnent incontestablement la mesure de l'obligation qui leur serait faite s'ils étaient tenus de conserver pendant une durée d'un an trace de l'ensemble des connexions et du coût que représenterait, alors, la recherche de celles des données qui pourraient, le cas

[1] *Cf.* le 6e rapport d'activité de la CNIL pour 1985, p. 66 à 68.

échéant, être utiles à une enquête. Il serait à craindre que le coût final d'une telle obligation soit reporté sur les internautes. — L'appréciation de la Commission

L'obligation faite aux fournisseurs d'accès de conserver à des fins de police trace des connexions qui, par recoupement avec d'autres données, peuvent dévoiler notre navigation sur le Web et, de manière plus générale, l'usage privé que l'on fait du réseau, déroge aux principes fondamentaux de protection des libertés individuelles. Dès lors, il convient que la loi édictant une telle obligation soit à la fois claire et précise et que le dispositif mis en œuvre soit adapté et proportionné.

Or, le projet de loi renvoie au pouvoir réglementaire le soin de déterminer les données en cause et leur durée de conservation précise, dans la limite maximale d'un an. Certes, la rédaction du projet de loi sur ce point laisse penser que la durée de conservation finalement retenue pourrait être, dans certains cas, inférieure à un an et que seules certaines données de connexion, et non pas toutes, seraient en définitive conservées. Cependant, l'hypothèse d'un tri entre des données à caractère technique qui sont rassemblées dans des fichiers dits « fichiers log » peut paraître assez peu réaliste d'autant qu'un tel dispositif reviendrait à ajouter à la contrainte faite aux opérateurs de conserver des données sans utilité pour eux une deuxième contrainte consistant à leur demander de procéder à une sélection a *priori* entre les données produites par la technologie. D'autre part et surtout, l'obligation ainsi instituée dérogeant au droit commun, sa portée et ses modalités de mise en œuvre paraissent devoir être déterminées par le législateur. Il est en tout cas permis de s'interroger sur le point de savoir si un renvoi aussi général au pouvoir réglementaire, fût-ce après avis de la CNIL, offre les garanties de précision et de clarté exigées dans une matière qui touche aux libertés individuelles et publiques, étant observé qu'il ne s'agit plus, comme dans la loi du 1er *août* 2000, de permettre l'identification d'auteurs de contenus diffusés sur Internet mais toutes les personnes se connectant à Internet.

Sur le fond, la Commission estime que dans la mesure où la pratique des fournisseurs d'accès n'est pas aujourd'hui harmonisée et où certains d'entre eux ne conservent que très peu de temps les données de connexion, ce qui au demeurant ne peut que fragiliser la sécurité informatique de leurs propres installations, l'obligation nouvelle qui serait désormais faite à l'ensemble des fournisseurs d'accès de conserver les données de connexion pendant une durée de trois mois serait adaptée aux objectifs d'intérêt public poursuivis par le projet de loi.

La Commission croit devoir souligner que, selon le témoignage recueilli auprès de ses homologues européens, ceux des États-membres ayant prévu une obligation de conservation de ces données pendant une durée maximale de cet ordre ne paraissaient pas avoir rencontré de problèmes particuliers en matière de lutte contre la délinquance par le réseau.

Par ailleurs, dans une résolution législative portant avis du Parlement européen sur le projet d'action commune relative à la lutte contre la pornographie enfantine sur Internet[1] cette assemblée a estimé qu'une durée de conservation des données de trafic de trois mois pouvait être adaptée.

[1] JO C219 du 30 iuillet 1999, p. 68 et p. 71.

Enfin, la Commission européenne, saisie pour avis par la Belgique d'un projet de loi de réforme du code pénal qui retenait, notamment, une durée de conservation des données d'appels et d'identification des utilisateurs d'au moins douze mois, et qui renvoyait à des arrêtés royaux le soin d'arrêter les durées de conservation précises en fonction des services utilisés, a émis un avis circonstancié estimant que l'obligation ainsi définie était insuffisamment précise au regard des exigences européennes, qu'elle constituait une restriction excessive à l'exercice des activités économiques et une atteinte non justifiée aux principes de protection des données personnelles.

L'ensemble de ces considérations conduit la CNIL à estimer qu'un délai de conservation de trois mois serait parfaitement proportionné et adapté aux intérêts en cause.

Enfin, les conditions dans lesquelles de telles données personnelles pourraient être saisies cessibles dans le cadre d'une procédure judiciaire mériteraient sans doute d'être précisées compte tenu de la nature particulière de telles données qui ne sont pas conservées par les personnes concernées par la communication, mais par un tiers (le fournisseur d'accès). En effet, le projet de loi, en son état, ne parait subordonner un tel accès à ces données à aucune condition tenant à la gravité de l'infraction recherchée et donne à penser que ces données pourraient être consultées ou saisies dans le cadre d'une enquête préliminaire qui se caractérise, pourtant, par le fait qu'à ce stade l'infraction n'est pas patente et ne permet pas à la police judiciaire de procéder à des saisies ou perquisitions, sans l'accord exprès des personnes concernées.

La publicité par voie électronique (articles 25 et 26 du projet de loi)

Le dispositif prévu

Le titre III « Du commerce électronique » comporte un chapitre II relatif à la publicité par voie électronique qui institue une obligation de transparence à l'égard des consommateurs par l'identification claire et non équivoque de la nature publicitaire des messages électroniques de publicité non sollicitée ainsi que des offres promotionnelles telles que les rabais, primes, cadeaux, concours ou jeux. Cette obligation est tout à fait satisfaisante.

Le projet de loi introduit par ailleurs dans le code de la consommation un article L. 121-15-3 nouveau faisant obligation aux personnes physiques ou morales utilisant la messagerie électronique des internautes pour leur adresser des messages publicitaires qu'ils n'ont pas sollicités de « veiller » à ce que de tels messages « ne soient pas adressés à des personnes physiques qui ne souhaitent pas recevoir ce type de communication et qui se sont inscrites à cet effet dans des registres d'opposition ». Le projet de loi renvoie à un décret en Conseil d'État le soin de fixer les conditions de fonctionnement de tels registres.

Les *enjeux*

Cette dernière disposition appelle plusieurs observations.

Elle tranche un débat auquel tous les internautes dans tous les pays sont extrêmement sensibles puisqu'il met en cause, à la fois, la nature d'Internet dont il paraît souhaitable qu'il ne soit pas considéré comme un outil à vocation exclusivement marchande, le sort des données personnelles et tout particulièrement l'utilisation à des fins commerciales des adresses électroniques que les internautes ont pu communiquer à de toutes autres fins dans les espaces publics de l'Internet (forum de discussion, liste de diffusion, etc.) et enfin

la tranquillité de ceux qui peuvent souhaiter ne pas voir leur boîte aux lettres électronique inondée de messages indésirables, sans avoir à accomplir de démarche particulière à cet effet.

Ce débat qui s'est focalisé autour de ce que l'on nomme communément le *« spamming »* qui est la forme la plus controversée du publipostage électronique et qui consiste à adresser des messages électroniques à des centaines, des milliers, voire des millions de destinataires avec lesquels l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet, est beaucoup plus important qu'il n'y paraît.

En effet, le publipostage électronique ne concerne pas le seul commerce électronique. Il peut être le support de communication de messages de nature très différente : prosélytisme religieux ou sectaire, messages à caractère pornographique, etc. Par ailleurs, les adresses électroniques des internautes ne sont pas toutes celles de personnes majeures : des mineurs peuvent être concernés.

Aussi convient-il que la règle de droit qui sera posée en la matière puisse prévenir toute dérive. En n'évoquant que la seule publicité commerciale, et en faisant obligation aux internautes ne souhaitant pas être sollicités de s'inscrire sur des registres d'opposition, le projet de loi dans sa rédaction actuelle pourrait laisser penser que serait régulier tout envoi de message non sollicité, quelle qu'en soit la nature, à l'égard d'une personne, quel qu'en soit l'âge, qui ne se serait pas inscrite dans un registre d'opposition. Une telle manière de voir, si elle devait prospérer, pourrait avoir des effets tout à fait désastreux, compte tenu notamment du nombre de jeunes adolescents disposant d'une adresse électronique.

Par ailleurs, la prospection électronique tire sa force des caractéristiques particulières d'Internet qui doivent être prises en compte au moment de légiférer sur le sujet. En effet, à la différence de la prospection traditionnelle, dans laquelle l'expéditeur supporte entièrement les frais de prospection (qu'elle soit postale, téléphonique ou par télécopie), la prospection électronique est quasiment à coût nul pour le prospecteur. Il est possible de se procurer sur Internet pour des sommes modiques des CD-Rom concernant jusqu'à 60 millions d'adresses électroniques. Les frais de production et de communication des messages sur Internet sont, grâce à la numérisation et aux possibilités de duplication immédiate qu'autorise la technologie, sans commune mesure avec les coûts élevés que nécessitent les envois postaux (fabrication de maquette, coût du papier, mise sous pli, affranchissement). Or, jusqu'à présent, le législateur, national ou européen, a toujours considéré que plus le coût de la prospection était faible pour le commerçant, plus les risques d'abus étaient réels, comme l'ont manifesté, tour à tour, la prospection téléphonique par automate d'appels (dans les années 80) et surtout la prospection par télécopie (dans les années 90).

C'est la raison pour laquelle l'Union européenne s'est accordée pour limiter l'usage de telles formes de prospection en subordonnant l'utilisation des automates d'appels et, désormais, de la télécopie à des fins de prospection au consentement de la personne concernée : sans consentement, ces modalités de prospection sont irrégulières.

Enfin, et surtout, le problème traité par le projet de loi ne se limite pas aux inconvénients qui s'attacheraient à la seule réception d'un message non sollicité par l'internaute. Il ne peut y avoir sur Internet d'envoi de messages que s'il y a eu précédemment collecte automatisée des adresses électroniques des in-

ternautes, c'est-à-dire, constitution de véritables bases de données dont l'ampleur a été soulignée ci-dessus. Telle est la pratique de certains opérateurs qui n'hésitent pas à lancer des robots sur Internet afin de récupérer toutes les adresses électroniques disponibles sur les espaces publics d'Internet. Dès lors, l'adresse électronique utilisée, et éventuellement le « profil » de son titulaire tel qu'il peut être déduit des échanges que l'internaute considéré a pu librement avoir sur tel sujet particulier dans un forum de discussion, sont conservés, à son insu dans une base de données, à des fins commerciales ou de prosélytisme, par un tiers avec lequel il n'a jamais eu de contact. Soutenir que la mise en place de registres d'opposition constituerait une mesure suffisante revient à espérer qu'en évitant d'alarmer l'internaute, ce dernier n'exercera aucun des droits qui lui sont pourtant reconnus à l'égard des traitements de données personnelles le concernant : les données le concernant continueront à être traitées et, le cas échéant, cédées à des tiers mais, tenu dans l'ignorance du fait, il ne disposera plus d'aucun moyen de demander la radiation de ses coordonnées des fichiers dans lesquels elles figurent.

Au regard de ces trois caractéristiques, qui distinguent clairement la prospection électronique sur Internet d'autres formes plus classiques de prospection commerciale, on ne peut que s'interroger sur les justifications du dispositif prévu dans le projet de loi.

Sans doute la directive européenne 2000/31 dite « Commerce électronique », prévoit-elle la mise en place de tels registres d'opposition. Mais, contrairement à ce que soutiennent certains groupes professionnels, cette directive n'a aucunement entendu choisir entre les deux solutions qui ont été passionnément discutées sur le sujet, la première consistant à permettre que toute prospection électronique soit possible à l'égard des personnes qui n'auraient pas manifesté, par un geste positif, leur refus d'en recevoir (dite *« opt out »),* la deuxième soutenant au contraire que, compte tenu de ses caractéristiques, la prospection par courrier électronique était une des plus intrusives qui soient dans le monde du commerce et qu'il convenait, comme pour la publicité par automates d'appels ou par télécopie, d'en subordonner l'usage aux seules personnes qui y avaient consenti (dite *« opt in »).* En effet, l'article 7 de la directive concernée n'évoque que « les États membres qui autorisent les communications commerciales non sollicitées », signifiant ainsi clairement que le choix d'autoriser ou non de telles formes de publicité relevait du niveau national et n'était nullement imposé par la législation communautaire. La rédaction de cet article fait en outre une référence expresse aux « autres exigences prévues par le droit communautaire » parmi lesquelles figure la directive « protection des données personnelles » du 24 octobre 1995, le considérant 30 du texte européen précisant par ailleurs que « la question du consentement du destinataire pour certaines formes de communications commerciales non sollicitées n'est pas traitée par la présente directive ». Dès lors aucun argument tenant aux exigences communautaires n'impose à la France d'arrêter un tel dispositif.

L'appréciation de la Commission

La Commission ne peut, dans ces conditions, que rappeler les conclusions qu'elle a rendues publiques dans son rapport d'ensemble sur le sujet, adopté le 14 octobre 1999[1]

[1] Rapport, *Le publipostage électronique et la protection des données personnelles,* adoptée par délibération du 14 octobre 1999-www.cnil.fr

Outre les caractéristiques particulières de la prospection électronique qui ont été rappelées plus haut, la Commission souhaite souligner, qu'à la différence des autres formes de prospection, la prospection par courrier électronique est très « intrusive » et directement ciblée. Une boîte aux lettres électronique, à la différence d'une « boîte aux lettres physique », est directement ouverte sur le monde et dépourvue des « barrières » que constituent un hall d'entrée, un digicode ou une gardienne.

Par ailleurs, ce mode de prospection est coûteux pour les internautes, un récent document d'étude de la Commission européenne[1] l'évaluant à 10 milliards d'euros le coût annuel mondial supporté par eux au titre de la réception de messages non sollicités (le coût étant déterminé en fonction de la durée moyenne de lecture des messages avant effacement).

C'est la raison pour laquelle la pratique du *« spam »* est vécue, par les internautes mais aussi par les fournisseurs d'accès à Internet dont les installations peuvent être utilisées à leur insu pour dupliquer un même message à des milliers d'exemplaires — encombrant ainsi, au détriment des usagers, le volume de la bande passante et donc la rapidité des connexions — comme une pratique intolérable.

Aussi, certains pays européens ont-ils subordonné l'usage de (a prospection non sollicitée par courrier électronique, comme c'est déjà le cas pour la prospection par automates lanceurs d'appels ou par télécopie, au consentement des personnes. Telle est déjà la norme dans les deux pays européens qui connaissent le plus fort taux de pénétration de l'Internet grand public (Finlande et Danemark) ainsi qu'en Allemagne et en Autriche.

En outre, les acteurs professionnels qui sont nés avec l'Internet et qui perçoivent sans doute mieux que d'autres les attentes et les exigences des internautes à l'égard des bonnes pratiques sont très majoritairement favorables à la solution du « consentement » *(opt in)* qui, à leurs yeux, présente un considérable avantage en terme de communication commerciale dans la mesure où, à la différence des registres d'opposition *(opt out)* qui ne permettent de communiquer qu'à partir de souhaits inexprimés, les listes compilées d'adresses de personnes « consentantes » exprimeraient une « multitude de désirs de consommation et de centres d'intérêts précis » à valeur ajoutée marchande beaucoup plus élevée. C'est en tout cas ce qui résulte de l'étude des pratiques les plus récentes aux États-Unis à laquelle a procédé la Commission européenne[2].

Pour sa part, la CNIL souhaite que le débat qui s'engagera sur ce sujet permette d'établir une règle claire, de nature à assurer la confiance et le respect des droits des internautes, alors que les dispositifs arrêtés par plusieurs directives européennes paraissent sur ce point contradictoires.

Aussi, convient-il d'en revenir aux principes généraux posés par la directive européenne du 24 octobre 1995 :
— toute collecte de données opérée dans un espace public de l'Internet, sans le consentement des personnes concernées, doit être considérée comme irrégulière et déloyale ;

[1] *Communications commerciales non sollicitées et protection des données,* Internai Market DG, octobre 2000.
[2] Rapport déjà cité, Internai Market DG.

— toute personne (client ou visiteur du site) doit pouvoir s'opposer en ligne à une utilisation commerciale de ses données ou à une cession commerciale des données ainsi collectées à un tiers, à des fins de prospection commer ciale.

Une telle manière de voir n'est en rien contraire aux intérêts du commerce électronique puisqu'elle permettrait à tout commerçant en ligne de recourir à la messagerie électronique pour adresser des offres ou propositions nouvelles à l'ensemble de ses clients ou des visiteurs du site, dès lors que ces derniers auraient été préalablement informés, par une mention en ligne, d'une telle éventualité et de leur possibilité de s'y opposer, comme l'exigent d'ailleurs les règles ordinaires de protection des données personnelles et comme le pratique déjà l'ensemble des professionnels dans le monde hors ligne.

Elle permettrait également aux professionnels de céder leurs fichiers de clients ou de prospects, ou d'utiliser le fichier d'un tiers mis à leur disposition, dès lors que les adresses électroniques ainsi utilisées, cédées ou acquises, concerneraient des personnes ayant été préalablement informées de telles cessions ou de tels usages, et de leur droit de s'y opposer.

La solution préconisée par la Commission interdirait en revanche clairement deux pratiques :
— la collecte massive (et à l'insu des personnes concernées) d'e-mail dans les espaces publics de l'Internet où l'on peut souhaiter avoir un échange au sein d'une communauté partageant un même sujet d'intérêt sans que son adresse ou ses propos soient immédiatement exploités par un tiers à des fins étrangères au forum ou à la liste de discussion ;
— la cession de données personnelles collectées par un site A à un tiers lorsque les internautes ayant communiqué leur adresse électronique au site A n'ont pas été informés de l'éventualité d'une telle cession et mis en mesure de s'y opposer, aussitôt et en ligne.

De nombreux organismes de labellisation de sites commerciaux s'engagent déjà à respecter de telles recommandations. Tel est notamment le cas de L@belsite et du bureau Veritas. On comprend mal que la loi sur la société de l'information ne soit pas mise à profit pour consacrer ces « bonnes pratiques » loin de tout débat, un peu dogmatique, entre le « *opt in* » et le *« opt out ».*

Aussi, un principe général d'interdiction de collecte des adresses électroniques ou de toute autre donnée personnelle à partir des espaces publics de l'Internet, sans le consentement des internautes, devrait-il être posé par la loi. Toute collecte irrégulière d'adresse électronique dans ces conditions devrait être sanctionnée d'une amende par adresse, une disposition de cette nature paraissant mieux adaptée et plus dissuasive que les dispositions générales de l'article 226-18 du code pénal qui sanctionne la collecte frauduleuse ou déloyale d'une peine de cinq ans d'emprisonnement.

Cette proposition n'exclut nullement la mise en oeuvre de registres d'opposition que le projet de loi envisage et dont certains sont déjà mis en œuvre par des organisations professionnelles. Mais elle leur conférerait, alors, la nature d'ultime « filet de sécurité » qui doit être la leur, comme dans le monde du commerce hors-ligne.

Cette proposition serait conforme au socle de garanties reconnues en la matière par l'ensemble de l'Union européenne et de nature à prévenir les effets du *« spamming »* en Europe.

L'accès aux données publiques (articles 3 à 6 du projet de loi)

Observations liminaires

Sous un même intitulé le chapitre II du titre I[er] du projet de loi regroupe des dispositions de nature et de portée différentes : les premières sont principalement destinées à faciliter l'accès du citoyen aux informations détenues par l'État ou les collectivités publiques (les données sont alors dites « publiques » parce qu'elles sont collectées ou produites dans le cadre d'une mission de service public) ; les secondes posent un principe général de gratuité et une obligation de mise en ligne sur Internet de l'ensemble des actes et décisions pris dans le cadre d'une mission de service public soumis à une obligation de publicité en vertu de dispositions législatives ou réglementaires (les données sont alors dites « publiques » parce qu'il s'agit de données soumises à un certain régime de publicité).

Une telle présentation ne facilite pas la compréhension des champs d'application (respectifs ou bien se recouvrant pour partie) des deux séries de dispositions.

Le souci d'une plus grande accessibilité de l'information administrative et celui de favoriser les activités économiques liées à la valorisation de l'information administrative ne peuvent qu'être partagés. À cet égard le projet de loi prolonge, à l'heure de la société numérique, la volonté de plus grande transparence que le législateur a manifestée en adoptant la loi du 17 juillet 1978 portant diverses mesures d'améliorations des relations entre l'administration et le public, laquelle a d'ailleurs été modifiée récemment, par une loi du 12 avril 2000, dans le souci de mieux harmoniser ses dispositions avec les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'article 3 du projet de loi n'appellera dès lors que des observations d'ordre juridique et technique.

Tel n'est pas le cas de l'article 4 du projet dont le dispositif d'ensemble, pris dans sa généralité, appelle des observations de fond.

Sur l'obligation de mise en ligne sur Internet de l'ensemble des actes et décisions pris dans le cadre d'une mission de service public, soumis à une obligation de publicité (article 4 du projet)

— Le dispositif prévu

L'article 4 du projet de loi fait obligation à l'ensemble des services de l'Etat et des établissements publics à caractère administratifs de mettre à la disposition du public, sur des sites Web accessibles en ligne gratuitement, les données essentielles qui les concernent parmi lesquelles figure « l'ensemble des actes et décisions [...] qui sont soumis à une obligation de publicité en vertu de disposition législative ou réglementaire ».

Un décret en Conseil d'État pris après avis de la CNIL « peut » déterminer les actes et les décisions échappant à l'obligation de mise en ligne « en raison des risques particuliers que leur utilisation par des tiers pourrait faire peser sur les libertés individuelles». Le projet prévoit en outre que la mise en œuvre d'un traitement automatisé de données à caractère personnel préalablement diffusées en ligne est « soumise aux règles posées par la loi du 6 janvier 1978 ».

Il résulte clairement de l'ensemble de ce dispositif que dès lors qu'un acte ou une décision (y compris ceux revêtant un caractère nominatif) sera considéré comme « donnée essentielle », sa mise en ligne obligatoire sera de droit, sauf exception posée par décret en Conseil d'Etat après avis de la CNIL.

— Les enjeux

Au regard de la protection des données personnelles et de la vie privée, on peut s'interroger sur le point de savoir si, d'une part, dans la généralité de ses termes, l'obligation qui serait faite de diffuser sur Internet toute donnée « publique », y compris des données personnelles, a suffisamment pris en compte les spécificités liées à un mode de diffusion tel qu'Internet et, d'autre part, si la réserve faite, par exception, pour certains actes et décisions, au motif de risques particuliers que leur utilisation pourrait faire peser sur les libertés individuelles, constitue une garantie suffisante.

En effet, la diffusion d'une information sur Internet réalise un changement d'échelle tout à fait considérable. Toute information diffusée sur Internet devient accessible au plan mondial, et, surtout, les possibilités de duplication et de capture de l'information sont sans limite et ne peuvent être contrôlées. Ainsi, non seulement un site d'information peut être copié à l'infini et stocké sur une multitude de serveurs informatiques sans que le responsable de la diffusion initiale le sache, mais il est également possible, grâce aux prouesses des moteurs de recherche, d'accéder à l'information sans même connaître l'existence du site de diffusion.

Ainsi suffit-il d'indexer le nom d'une personne physique sur un moteur de recherche pour obtenir l'ensemble des informations la concernant diffusées sur Internet à partir de sites géographiquement épars ou de nature différente. Ce qui est techniquement possible lorsqu'une recherche documentaire via Internet est entreprise sur Rabelais, l'est aussi lorsqu'il s'agira de se renseigner sur un candidat à l'emploi ou à un logement, sur un voisin ou un proche, sur un demandeur au crédit, et ce, à l'insu des personnes concernées.

Souligner ces caractéristiques techniques manifeste qu'au-delà des « risques particuliers » qu'une telle diffusion d'informations nominatives est susceptible de présenter au regard des libertés individuelles, et qui justifieraient alors le dispositif d'exception par décret en Conseil d'État pris après avis de la CNIL, la diffusion d'une information se rapportant à une personne physique génère un risque « très ordinaire » mais permanent — dès lors qu'il peut suffire d'une diffusion de quelques minutes sur Internet pour générer la duplication et la conservation de l'information en cause, sans limite contrôlable de durée et sur une multitude de serveurs — de réutilisation des informations à l'insu des personnes concernées et étrangère à la finalité de publicité qui a pu, un instant, être recherchée.

Pour n'évoquer que quelques exemples « d'actes ou de décisions pris au nom d'une personne publique qui sont soumis à une obligation de publicité en vertu de dispositions législatives ou réglementaires » et qui devraient, à suivre le projet de loi, être mis en ligne par les administrations ou collectivités publiques concernées, sauf intervention d'un décret dérogatoire en Conseil d'Etat : un jugement portant sur un licenciement pour faute grave, un homicide involontaire, la responsabilité professionnelle d'un praticien, un contentieux fiscal, etc., est naturellement soumis à une obligation de publicité, de même que le rôle des impôts (articles L. 104 et L. 111 du Livre des procédures fiscales), la liste électorale qui comporte la date de naissance et

l'adresse personnelle des personnes (article L. 28 du code électoral), les bans de mariages qui comportent la profession et le domicile des futurs époux (article 63 du code civil), le cadastre dont la publicité est organisée par l'article 37 du décret de valeur législative du 7 messidor An II, les permis de construire (article R. 421-39 du code de l'urbanisme).

Certes, de tels documents sont déjà publics ou communicables aux personnes intéressées.

Mais la publicité jusqu'alors organisée autour de tels actes ou décisions peut poursuivre une finalité particulière ou être assortie de réserves d'usage dont le respect ne pourrait plus être assuré si ces actes et décisions étaient accessibles en ligne. Ainsi la consultation des listes électorales est libre mais il ne peut en être fait une utilisation à des fins exclusivement commerciales, le rôle de l'impôt sur le revenu est consultable à la direction des services fiscaux mais par les seuls contribuables qui relèvent de sa compétence territoriale (le Livre des procédures fiscales précisant de surcroît que la publication ou la diffusion par tout autre moyen est interdite sous peine d'amende fiscale), la publicité dont est assortie la délivrance des permis de construire cesse dès la in du chantier, celle des bans de mariages est exclusivement justifiée par le souci de permettre d'éventuelles oppositions à mariage, celle des décisions de justice par celui de manifester l'impartialité du tribunal et de restituer dans leurs droits toutes les personnes concernées par la décision rendue.

Ces réflexions ne signifient pas qu'il conviendrait pour autant de proscrire toute accessibilité par Internet de telles informations. Ainsi, dans certains cas, la technique peut venir au soutien des précautions à prendre : il pourrait être envisagé, à titre d'exemple, que le cadastre puisse être accessible par Internet dès lors que serait mis en place un système d'accès par cartographie permettant, pour un bien immobilier particulier, d'en connaître le propriétaire. À défaut d'une telle précaution, dont il conviendrait de s'assurer techniquement de l'effectivité, on transformerait un registre de propriétés (à qui appartient cette parcelle que je souhaite acheter ?) en une liste de propriétaires (quels sont les biens que possède Monsieur X ?).

Mais le souci de précaution appelle assurément à un strict encadrement de la diffusion sur Internet d'informations nominatives. Ainsi, le Gouvernement a exclu de la diffusion du Journal officiel sur Internet les décrets de naturalisation afin que la publicité dont sont assortis ces décrets, qui s'apparente à une mesure de bienvenue dans la communauté nationale, ne se transforme pas en menace pesant sur les intéressés, par les possibilités de recherche et de capture de telles informations que peut offrir Internet à certains groupes ou officines de leur pays d'origine. Dans le même esprit, la CNIL mène depuis plusieurs mois une large concertation avec les diffuseurs publics et privés de jurisprudence sur Internet afin d'apprécier les mesures propres à éviter tout détournement de finalité des bases de données des décisions de justice, initialement conçues à des fins exclusives de recherche documentaire, mais qui pourraient se transformer aisément, accessibles gratuitement sur Internet en comportant le nom et quelquefois l'adresse des parties, en véritables bases de renseignements sur les personnes.

En tout état de cause, au-delà de précautions toujours possibles, c'est une certaine retenue dans la diffusion d'informations nominatives qui s'impose, dans le souci de la protection et de la tranquillité des personnes concernées, alors surtout que le projet de loi s'efforce de régler un long contentieux entre

l'État et les diffuseurs privés qui ne porte que très marginalement sur des données à caractère nominatif.

— L'appréciation de la Commission

Pour l'ensemble de ces motifs la Commission souhaite que, s'agissant des données essentielles revêtant un caractère nominatif, le projet puisse inverser le principe (mise en ligne) et l'exception en limitant l'obligation de mise en ligne des données essentielles aux seuls les actes, et décisions ne revêtant pas de caractère nominatif, un décret en Conseil d'État pris après avis de la CNIL pouvant déterminer ceux des actes et décisions à caractère nominatifs qui pourraient obéir au nouveau régime juridique des « données essentielles ».

Au demeurant une telle suggestion paraît seule conforme aux dispositions de la directive du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données qui n'exclut nullement de son champ d'application les données à caractère personnel revêtant ou ayant revêtu un caractère public, se bornant à ménager quelques exceptions de portée limitée (exception à l'obligation de notification des traitements et exception à l'exigence de subordonner les flux transfrontières de données aux seuls pays disposant d'un niveau de protection adéquat pour les registres qui, en vertu de dispositions législatives ou réglementaires sont destinés à l'information du public et ouverts à la consultation du public). Ces dérogations n'ont ni pour objet ni pour effet de priver les personnes concernées des droits fondamentaux qu'elles tiennent des législations de protection des données personnelles : droit d'opposition à une utilisation commerciale de données, droit de contrôle de la finalité des traitements mis en oeuvre.

Sur l'obligation de mise à disposition des données numérisées collectées ou produites dans le cadre d'une mission de service public (article 3 du projet)

— Le dispositif prévu

Le projet de loi crée une obligation nouvelle aux personnes publiques et aux personnes privées chargées d'une mission de service public : celle de mettre à la disposition du public les données qu'elles collectent ou qu'elles produisent.

À la différence du dispositif déjà prévu par la loi du 17 juillet 1978 qui, dans son article 10, interdit « la possibilité de reproduire, de diffuser ou d'utiliser à des fins commerciales les documents communiqués », le public ou les diffuseurs privés qui pourront accéder à des données sur le fondement de ces dispositions nouvelles, pourra les exploiter pour son propre compte, les utiliser, les diffuser y compris à des fins commerciales, sous réserve de conclure une convention avec la personne ou l'administration détentrice des données, cette mise à disposition pouvant donner lieu à perception d'une redevance.

Seront exclues d'une telle mise à disposition les données qui ne sont pas communicables à d'autres personnes que la personne concernée en application de la loi du 17 juillet 1978, modifiée par la loi du 12 avril 2000, soit les données suivantes :

— les documents administratifs dont la consultation ou la communication porterait atteinte au secret des délibérations du Gouvernement et des autori tés responsables du pouvoir exécutif, au secret de la défense nationale, à la conduite de la politique extérieure de la France, à la sûreté de l'État, à la sé curité publique ou à la sécurité des personnes, à la monnaie et au crédit pu-

blic, au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, à la recherche, par les services compétents, des infractions fiscales et douanières, ou, de façon générale, aux secrets protégés par la loi ;

— les documents administratifs dont la communication porterait atteinte au secret de la vie privée et des dossiers personnels, au secret médical et au se cret en matière industrielle et commerciale ;

— les documents portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable ou fai sant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice.

Le projet de loi précise que la mise à disposition des données à caractère personnel devra s'effectuer dans le respect des règles posées par la loi du 6 janvier 1978.

— Les observations de la Commission

Elles portent principalement sur l'articulation de l'article 3 du projet avec la loi du 17 juillet 1978 modifiée par la loi du 12 avril 2000 et la loi du 6 janvier 1978.

En effet, la loi du 12 avril 2000 avait principalement pour objet de mieux harmoniser les dispositions des deux lois de 1978 dans le souci que l'informatisation de l'administration ne la conduise pas à invoquer la loi « informatique et libertés » pour refuser de communiquer à un tiers un document administratif comportant des informations nominatives, au sens de la loi du 6 janvier 1978, au motif que ce document serait informatisé.

Aussi, suivant en cela les suggestions de la CNIL et du Conseil d'État, le législateur a-t-il entendu que l'on ne puisse pas opposer une loi à une autre : le titulaire du droit de communication à l'information administrative est considéré comme un « tiers autorisé » à avoir accès à un traitement, sans que la finalité de ce dernier puisse être opposée à l'exercice de ce droit à la transparence administrative (article 29-1 nouveau de la loi du 6 janvier 1978). Encore convient-il de relever que cet accès ne peut, sur le fondement de ces récentes dispositions, qu'être ponctuel, l'article 10 de la loi du 17 juillet faisant de surcroît interdiction au titulaire du droit de communication de « reproduire, diffuser ou d'utiliser à des fins commerciales les documents ainsi communiqués ».

À cet égard, le projet de loi change la donne puisqu'il paraît ajouter au droit individuel et ponctuel de demander communication d'un document administratif, fût-il numérisé, une obligation générale de mise à disposition de tout document communicable en application de la loi du 17 juillet 1978.

Le problème de coordination entre ces diverses lois serait moins aigu si les informations nominatives étaient exclues du dispositif. Mais, précisément, des informations nominatives peuvent se trouver en cause. Certes, sont considérées comme relevant des exceptions prévues par la loi du 17 juillet 1978 au titre du secret de la vie privée, et à ce titre non communicables à un tiers, la date de naissance, l'âge, la situation familiale, la situation matrimoniale et patrimoniale, l'adresse personnelle, le numéro de téléphone, la formation et les origines professionnelles, le numéro INSEE, les numéros d'immatriculation des véhicules de victimes et de témoins d'accidents.

En revanche, sont communicables, en application de la loi du 17 juillet 1978, l'adresse administrative, l'indice de rémunération, le grade et l'éche-

lon des fonctionnaires et autres agents publics, la liste des commerçants d'une commune avec les montants de la taxe professionnelle acquittée par chacun, la liste des sous-traitants d'un marché public et le montant des interventions effectuées. Aux termes du projet de loi, de tels documents devront désormais être tenus à la disposition du public qui en fait la demande.

Le projet de loi prévoit, certes, qu'une telle mise à disposition devra « s'effectuer dans le respect des règles posées par la loi du 6 janvier 1978 », ce qui constitue une utile garantie dans certaines hypothèses où la CNIL subordonne la diffusion de certaines informations statistiques, particulièrement sensibles mais sur de petits échantillons, pour éviter tout risque de ré-identification des personnes, directement ou indirectement par recoupement.

Mais, le dispositif d'ensemble manque singulièrement de clarté dans la mesure où il prévoit qu'en cas de désaccord entre la personne qui détient les données et celle qui en sollicite la communication, une instance, de médiation dont la composition est renvoyée à un décret en Conseil d'État pourra être saisie. Or, le projet envisage explicitement que le désaccord puisse porter soit sur la « nature des données communicables », ce qui aurait pu justifier l'intervention exclusive de l'autorité qui est naturellement chargée de porter une appréciation sur ce point (la Commission d'accès aux documents administratifs), soit sur « les modalités d'utilisation ou de diffusion des données », ce qui aurait pu justifier une intervention de la CNIL dans les cas où de telles données revêtiraient directement ou indirectement un caractère nominatif.

La création d'une instance ad *hoc* venant s'ajouter aux deux autorités précédemment citées ne contribue pas à clarifier le dispositif dans son ensemble.

Aussi, tout en partageant pleinement l'objectif général poursuivi par le texte et l'intérêt qui s'attache à mettre à profit les possibilités offertes par la numérisation pour renforcer la transparence administrative et assurer un plus efficace partage de l'information entre l'État et les diffuseurs privés, dans le respect de la vie privée des personnes, la Commission ne peut-elle que faire part de sa perplexité sur l'articulation des dispositions de l'article 3 du projet avec celles de la loi du 12 avril 2000.

L'accès aux archives publiques (articles 7 et 8 du projet)

Le dispositif prévu

Le projet de loi réaffirme le principe de libre communication des archives publiques quels que soient leur support, leur lieu, leur mode de conservation et réaménage et, de manière générale, raccourcit les délais spéciaux établis pour certains documents présentant un caractère particulier de confidentialité. Ainsi, le délai de droit commun de communicabilité de ces documents est ramené de 30 à 25 ans.

Le délai de communicabilité des documents dont la communication porterait atteinte au secret médical et ramené de 150 ans après la naissance à 25 ans après le décès ou, si la date du décès est inconnue, à 125 ans à compter de la naissance.

S'agissant des documents dont la communication porterait atteinte à la protection de la vie privée ou rendrait public une appréciation, un jugement de valeur ou le comportement d'une personne dans des conditions susceptibles

de lui nuire, le délai de libre communication est ramené de 60 à 50 ans à compter de la date du document, ou à 25 ans à compter de la date du décès de l'intéressé. Ces mêmes délais s'appliqueraient aux documents judiciaires. S'agissant des mineurs l'ensemble de ces délais serait prolongé à 100 ans à compter de la date du document.

S'agissant enfin des délais de communication des registres de l'état civil, le délai de 100 ans est maintenu pour les registres de naissances mais ramené à 50 ans pour les registres de mariages.

Des possibilités de dérogation sont aménagées permettant la consultation des documents protégés avant l'expiration des délais de libre communication lorsque « l'intérêt qui s'attache à la consultation de ces documents ne conduit pas à porter une atteinte disproportionnée aux intérêts que la loi a entendu protéger ». Le bénéficiaire de l'autorisation est alors tenu de ne publier et de ne communiquer aucune information recueillie dans les documents qui soit susceptible de porter atteinte aux intérêts protégés par la loi.

L'appréciation de la Commission

La libéralisation de l'ouverture des archives est considérée comme souhaitable depuis plusieurs années, de nombreux acteurs s'accordant à reconnaître que le dispositif actuel est, au moins dans certains cas, trop restrictif et les dérogations accordées, souvent discrétionnaires.[1]

La Commission croit cependant devoir souligner que l'informatisation des documents versés aux archives, les facilités d'exploitation des informations qu'elle permet et les usages possibles de telles exploitations par des tiers devraient appeler à une certaine prudence, hors le cas où les informations seraient traitées à des fins historiques, statistiques ou scientifiques. Mais précisément ces dernières hypothèses ont déjà conduit à modifier la loi du 6 janvier 1978 en autorisant la conservation des informations nominatives au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été initialement collectées ou traitées et leur traitement à des fins historiques, statistiques ou scientifiques. La loi du 12 avril 2000 a, en effet, modifié à cette fin l'article 28 de la loi « informatique et libertés ». Il résulte, en outre, de cette récente modification législative que tout traitement des données ainsi conservées à des fins autres qu'historiques, statistiques ou scientifiques devra être autorisé, à défaut d'accord exprès des intéressés, par la CNIL ou par décret en Conseil d'État sur proposition ou avis conforme de la CNIL.

L'articulation de ces récentes dispositions avec les dispositions du projet de loi soulève deux difficultés.

La première concerne la compatibilité entre un régime de liberté de communication d'archives, une fois les délais de libre communicabilité expirés, et un régime d'autorisation du traitement des données concernées.

La deuxième concerne le sens qu'il convient de donner à la notion de « personnes intéressées ». S'agit-il uniquement des personnes auxquelles les informations nominatives se rapportent ou, le cas échéant, de leurs ayant-droits ?

[1] les *archives de France,* rapport remis par M. Guy Braibant au Premier ministre le 28 mai 1996, La documentation Française, collections « Rapports officiels ».

Cette question est d'importance.

En effet, s'agissant tout particulièrement des informations dont le projet de loi précise qu'elles seraient susceptibles de porter atteinte à la protection de la vie privée ou de rendre publique le comportement d'une personne dans des conditions susceptibles de lui porter un préjudice ou encore des affaires portées devant des juridictions, les ayant-droits ne disposent-ils pas d'un droit légitime à ce que de telles informations ne puissent être révélées sans garantie pour la mémoire de leurs parents ou leur tranquillité personnelle ? A cet égard une libre communication, 50 ans après l'établissement du document ou 25 ans après le décès de la personne concernée, illustre le caractère pratique d'une telle interrogation.

S'agissant des données médicales, les progrès de la recherche génétique peuvent également donner à penser que la libre communication de telles données 25 ans après le décès de la personne concernée (qui, de surcroît, peut avoir décédé à un jeune âge) n'est pas sans soulever de difficultés. Il pourrait certes être soutenu que le régime d'autorisation aménagé par la loi du 12 avril 2000 pour les traitements de données archivées ne poursuivant pas une finalité historique, scientifique ou statistique est suffisant pour prévenir toute dérive. Cependant, aucune disposition du projet ne subordonne la communication des documents ou des traitements automatisés en cause à la délivrance préalable de cette autorisation de traitement. Que deviendraient de telles données, une fois communiquées à un tiers, si l'autorisation de les traiter n'était finalement pas accordée ?

La Commission croit devoir appeler l'attention sur l'ensemble de ces difficultés.

Il lui apparaît en définitive que les risques particuliers d'atteinte à la vie privée des personnes concernées ou à celle de leurs proches devraient conduire à clairement distinguer les délais et les procédures de communication de documents nominatifs, et plus encore de traitements automatisés de données personnelles, versés aux archives, lorsque la demande de communication ou de traitement de ces informations relève de la recherche historique, scientifique ou statistique.

Dans ces cas, une plus grande libéralisation de l'accès aux archives paraît tout à fait légitime sous la réserve qu'aucune information ainsi recueillie ou traitée puisse être diffusée, traitée ou communiquée à un tiers sous une forme individualisée ou susceptible de porter atteinte aux intérêts protégés par la loi. Seuls la notoriété de la personne en cause, le caractère historique ou public des faits devraient justifier une exception à ce dernier principe.

Dans les autres cas, compte tenu tout à la fois du fait que l'information archivée sera de plus en plus fréquemment numérisée et que les possibilités d'exploitation de cette information par des tiers s'en trouvera accrue (songeons à une diffusion de telles informations sur Internet ou à leur utilisation à des fins marchandes par des compagnies d'assurance, s'agissant des données médicales par exemple, ou bien encore de données à caractère personnel couvertes par le secret statistique), la Commission ne peut qu'émettre des réserves sur le dispositif prévu, sur ce point, par le projet de loi.

Délibération n° 01-019 du 15 mai 2001 relative à un projet d'arrêté portant création d'un traitement informatique de délivrance des visas dans les postes diplomatiques et consulaires mis en œuvre par le ministère des Affaires étrangères

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministre des Affaires étrangères d'un projet d'arrêté portant création d'un traitement informatique de délivrance des visas dans les postes diplomatiques et consulaires ;

Vu la Convention 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 Convention d'application de l'accord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes, signée le 19 juin 1990 ;

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° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que son décret d'application n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 79-18 du 3 janvier 1979 modifiée sur les archives ;

Vu l'arrêté du 20 juin 1989 portant création d'un traitement informatique de délivrance des visas dans les postes diplomatiques et consulaires ;

Vu l'arrêté du 8 mars 1996 portant création d'un traitement informatique des demandes de visa soumises à la consultation des autorités compétentes des Etats parties à la Convention de Schengen ;

Vu le projet d'arrêté du ministre des Affaires étrangères portant création d'un traitement informatique de délivrance des visas dans les postes diplomatiques et consulaires ;

Après avoir entendu Monsieur François Giquel, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

L'article 5-1 de l'ordonnance du 2 novembre 1945 modifiée relative aux conditions d'entrée et de séjour des étrangers en France dispose que tout étranger doit, pour entrer en France, être muni des documents et visas exigés par les conventions internationales et les règlements en vigueur. L'article 5 de la Convention d'application de l'accord de Schengen au 19 juin 1990, qui pose le principe de la libre circulation des personnes, mentionne la possession d'un visa comme l'une des conditions d'entrée sur le territoire des États Schengen, pour les ressortissants des États tiers qui n'en sont pas dispensés.

La délivrance des visas relève de la compétence des autorités consulaires françaises à l'étranger, placées sous l'autorité du ministre des Affaires étrangères. Pour faciliter la procédure d'instruction des demandes de visas par ses personnels, le ministère des Affaires étrangères a décidé, en 1986, de mettre en oeuvre un traitement informatique de délivrance des visas, le réseau mondial visas. Cette application, qui a reçu un avis favorable de la Commission, a depuis lors dû être adaptée aux modifications intervenues en

matière de délivrance des visas, en particulier lors de l'entrée en vigueur de la Convention d'application de l'accord de Schengen, qui a contraint les États signataires à adopter une politique commune relative à la circulation des personnes et à harmoniser leur politique en matière de visa, et a nécessité la mise en œuvre du réseau de consultation Schengen, soumis à l'avis de la Commission en 1995.
Le nouveau traitement dont la Commission est saisie par le ministère des Affaires étrangères constitue une refonte du réseau mondial visas.

1) La finalité du réseau mondial visas 2

Le traitement automatisé présenté par le ministère des Affaires étrangères a pour objet de « permettre l'instruction des demandes de délivrance des visas par les consulats et les sections consulaires des ambassades, en procédant notamment à l'échange d'informations avec le ministère de l'Intérieur et les autorités centrales des États Schengen ».

L'article premier du projet d'arrêté soumis à l'avis de la Commission précise qu'à cet effet, plusieurs fichiers sont mis en œuvre. Il s'agit :
— du fichier des demandes, délivrances et refus de visas, qui permettra de centraliser l'ensemble des demandes de visa, quelles que soient leurs modalités d'instruction et la décision prise par les autorités consulaires françaises (délivrance ou refus du visa) ;
— du fichier des répondants signalés, qui permettra d'enregistrer des données concernant des personnes physiques ou des organismes qui accueillent les demandeurs de visa lors de leur séjour en France. Les signalements opérés par les agents du ministère des Affaires étrangères pourront être favorables, lorsque toute garantie aura été apportée sur la « fiabilité » du répondant, ou défavorables, lorsqu'à l'inverse, des craintes existeront quant à la participation du répondant à des actions contraires aux dispositions relatives au séjour des ressortissants étrangers en France ;
— du fichier des titres de voyage répertoriés, qui comportera des données concernant des titres de voyage considérés irrecevables lors d'une demande de délivrance de visa (titres déclarés volés, perdus, annulés ou falsifiés) ;
— du fichier des interventions, qui permettra d'enregistrer les interventions dont l'objet est soit d'appuyer une demande de délivrance de visa, soit de solliciter le réexamen d'une demande à la suite d'une décision de refus ;
— du fichier des demandes de cartes de commerçant, qui permettra d'enregistrer des données concernant les personnes qui sollicitent une carte de commerçant et dont la demande doit être conjointe à celle de la délivrance d'un visa de long séjour ;
du fichier central d'attention, qui comportera des informations provenant du ministère des Affaires étrangères et du ministère de l'Intérieur. Les données fournies par le ministère de l'Intérieur concerneront les personnes enregistrées dans le système d'information Schengen sur le fondement de l'article 96 de la Convention d'application de l'accord de Schengen (non-admission) et les personnes inscrites dans le fichier des personnes recherchées au titre des catégories « TE » (opposition à entrée en France), « E11 » et « E12 » (étrangers faisant l'objet d'un arrêté ministériel d'expulsion du territoire français), et « IT » (ressortissants étrangers faisant l'objet d'une interdiction judiciaire du territoire). En outre, le ministère de l'Intérieur transmettra au ministère des Affaires étrangères une liste de personnes susceptibles de porter atteinte à la sûreté de l'État pour lesquelles il souhaite être consulté lorsque celles-ci sollicitent un visa ;

— des fichiers consulaires d'attention, qui enregistreront les signalements de personnes, favorables ou défavorables, effectués par les postes consulaires. Ces fichiers locaux, propres à chaque poste, pourront le cas échéant être communs à l'ensemble des représentations consulaires françaises d'un même pays ou d'une même zone géographique ;
du fichier du suivi du contentieux, qui permettra de suivre les recours introduits devant les juridictions par les demandeurs de visas déboutés.

2) Les informations enregistrées

Les informations enregistrées dans le réseau mondial visas 2 seront, outre les données figurant dans les fichiers d'attention, celles fournies par les personnes qui sollicitent la délivrance d'un visa lors du dépôt de leur demande (formulaire de demande, titre de voyage, justificatifs), complétées par des données concernant l'instruction de la demande. La liste exhaustive des données susceptibles d'être enregistrées sera annexée à l'arrêté portant création du réseau mondial visas 2.

S'agissant plus particulièrement des informations concernant le demandeur du visa, la Commission prend acte de ce que les informations relatives aux parents du demandeur ne seront recueillies que si les autorités grecques doivent être consultées au titre du partenariat instauré entre les États signataires de la Convention Schengen. De la même manière, les coordonnées de l'employeur du demandeur ne seront collectées que si le demandeur du visa ne réside pas dans le ressort du poste consulaire où la demande est déposée.

La Commission relève par ailleurs que le rapprochement qui peut être opéré entre la nationalité d'origine et le statut actuel du demandeur est susceptible de faire indirectement apparaître des informations relevant de l'article 31 de la loi du 6 janvier 1978. En conséquence, il appartient au ministère des Affaires étrangères de faire figurer sur tous les formulaires de demande de visa une mention satisfaisant aux prescriptions de l'article 31 alinéa premier, qui autorise la collecte de ces données sensibles dès lors que l'intéressé y consent de manière expresse.

S'agissant des informations concernant la demande de visa, la Commission relève qu'au titre du motif du séjour envisagé en France ou dans l'un des États signataires de la Convention Schengen, des informations à caractère médical pourront être enregistrées dans le réseau mondial visas 2. Compte tenu de la sensibilité de ces données et de la confidentialité dont elles doivent bénéficier, de la possibilité pour les personnels du ministère des Affaires étrangères chargés de la délivrance des visas de vérifier le bien-fondé de la demande au vu des justificatifs médicaux et, le cas échéant, de prendre l'attache de l'établissement d'accueil, la Commission estime que l'enregistrement dans le réseau mondial visas 2 de l'identité du médecin devant prodiguer les soins est excessif et non pertinent au regard de la finalité du traitement.

3) Les durées de conservation des informations

Les durées de conservation des informations qui seront enregistrées dans le réseau mondial visas 2 différeront selon leur objet.

Les informations enregistrées dans le fichier des demandes, délivrances et refus de visas seront conservées deux ou cinq ans, si un visa de court ou de long séjour est délivré. Cette durée de conservation n'appelle aucune observation de la part de la Commission.

En revanche, si la demande de délivrance de visa est refusée, le ministère des Affaires étrangères prévoit de conserver les informations pendant dix ans. Cette durée de conservation paraît excessive au regard de la finalité du traitement, la seule obligation pour le ministère des Affaires étrangères étant, aux termes de l'instruction consulaire commune applicable aux visas de court séjour, de conserver les informations, en cas de refus, au moins cinq ans. La Commission souhaite que la durée de conservation des informations relatives aux demandes de délivrance de visas refusées soit limitée à cinq ans. Cette durée n'emporte aucune conséquence sur l'archivage des informations qui ne présentent plus d'utilité administrative, qui sera alors soumis aux dispositions de la loi du 3 janvier 1979 modifiée sur les archives.

Le ministère des Affaires étrangères prévoit que les informations enregistrées au titre du fichier des interventions seront conservées dix ans. S'agissant de données qui concernent des demandes de délivrance de visas, leur durée de conservation devrait être celle de la durée la plus longue admise pour la gestion des demandes, soit cinq ans.

Les informations saisies dans le fichier des cartes de commerçant seront conservées cinq ans si le visa demandé est délivré, dix ans s'il est refusé. La Commission estime que, quelle que soit la décision prise par le ministère des Affaires étrangères, la durée de conservation de ces données ne doit pas excéder cinq ans.

Les données enregistrées au titre des contentieux seront conservées dix ans. La Commission estime sur ce point qu'il n'y a pas lieu de fixer a *priori* une durée de conservation spécifique, mais qu'en revanche, il convient de limiter la durée de conservation des informations à un an à compter de la date de la décision passée en force de chose jugée.

S'agissant des fichiers d'attention, le dossier soumis à l'avis de la Commission précise que les données relatives aux personnes signalées par le ministère des Affaires étrangères seront conservées 99 mois au maximum, que les intéressés fassent l'objet d'une fiche d'opposition ou soient enregistrés au titre *des* répondants signalés, que ce soit par l'administration centrale ou par un poste consulaire. Cette durée de conservation paraît excessive. La Commission demande que les informations enregistrées dans les fichiers d'attention ne soient pas conservées au-delà de cinq ans.

4) Les destinataires des informations

Aux termes de l'article 4 du projet d'arrêté, les destinataires des informations enregistrées dans le réseau mondial visas 2 seront, dans la limite de leurs attributions, les personnels du ministère des Affaires étrangères compétents en matière de délivrance des visas (personnels des consulats, des ambassades, de la direction des Français à l'étranger et des étrangers en France, du bureau des visas et des passeports diplomatiques, et, au sein du service du protocole, les sous-directions des privilèges et immunités diplomatiques et consulaires), la direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur, le service de la police de l'air et des frontières, les autorités centrales des États Schengen.

Cette liste de destinataires n'appelle aucune observation de la part de la Commission.

5) Les modalités d'exercice du droit d'accès

Le droit d'accès aux informations sera mixte.

Les informations enregistrées lors de la demande de visa feront l'objet d'un droit d'accès direct, qui pourra être exercé auprès du consulat ou de l'ambassade où la demande aura été déposée.

En revanche, les informations figurant dans les fichiers d'opposition ou d'attention, susceptibles de porter atteinte à la sûreté de l'Etat, la défense et la sécurité publique, feront l'objet d'un droit d'accès indirect, en application de l'article 39 de la loi du 6 janvier 1978.

La Commission prend acte de ce que les fichiers d'attention du ministère des Affaires étrangères (fichier central ou fichiers consulaires) pourront être vérifiés en application de ces mêmes dispositions, le ministère des Affaires étrangères s'étant engagé à prendre toutes mesures de nature à faciliter l'exercice du droit d'accès indirect par les membres de la CNIL, magistrats ou anciens magistrats, qui en ont la charge.

En outre, la Commission prend acte de ce que le ministère des Affaires étrangères s'est engagé à compléter les mentions figurant sur le formulaire de demande de visa, afin d'indiquer les destinataires des informations et de faire état de la possibilité d'exercer le droit d'accès en application de l'article 39 de la loi pour les informations figurant dans les fichiers d'attention.

6) Les mesures de sécurité

Les mesures de sécurité dont bénéficiera le réseau mondial visas 2 n'appellent aucune observation de la part de la Commission.

Prend acte de ce que :
— les données enregistrées dans le fichier central d'attention fournies par le ministère de l'Intérieur concernent des personnes qui figurent dans le fichier des personnes recherchées ou qui sont signalées dans le système d'informa tion Schengen sur le fondement de l'article 96 de la Convention d'applica tion de l'accord de Schengen ;
— le ministère des Affaires étrangères s'est engagé à compléter les men tions figurant sur les formulaires de demande de visa afin d'indiquer, d'une part, les destinataires des informations et, d'autre part, la possibilité d'exer cer le droit d'accès en application de l'article 39 de la loi du 6 janvier 1978 pour les informations figurant dans les fichiers d'attention.

Émet un avis favorable sur le projet d'arrêté sous réserve que :
— le ministère des Affaires étrangères fasse figurer sur l'ensemble des for mulaires de demande de visa une mention satisfaisant aux prescriptions de l'article 31 alinéa premier, qui subordonne la collecte de données faisant di rectement ou indirectement apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs des personnes au recueil de l'accord exprès des intéressés ;
— l'identité du médecin devant prodiguer les soins au demandeur d'un visa ne soit pas enregistrée dans le traitement ;
— la durée de conservation des informations relatives aux demandes de dé livrance d'un visa refusées, des informations enregistrées dans le fichier des interventions, des informations enregistrées dans le fichier des cartes de commerçant — que le visa de long séjour soit ou non délivré, des informa tions enregistrées dans les fichiers d'attention, qu'ils soient tenus par l'admi nistration centrale ou par les postes locaux, des informations enregistrées dans le fichier des répondants signalés, soit de cinq ans ;

— la durée de conservation des informations enregistrées dans le fichier des contentieux soit limitée à un an à compter de Ta date de la décision passée en force de chose jugée.

Délibération n° 01-020 du 15 mai 2001 portant avis conforme sur le projet de décret en Conseil d'Etat autorisant la création par le ministre de l'Intérieur d'un fichier des élus et candidats aux élections au suffrage universel et portant application des dispositions du 3e alinéa de l'article 31 de la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministre de l'Intérieur d'un projet de décret en Conseil d'Etat autorisant la création au ministère de l'Intérieur d'un fichier des élus et candidats aux élections au suffrage universel et portant application des dispositions du 3e alinéa de l'article 31 de la loi du 6 janvier 1978 ;

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

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, le décret n° 78-774 du 17 juillet 1978 pris ensemble ;

Vu la loi n° 79 -18 du 3 janvier 1979 sur les archives ;

Vu la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; Vu le code électoral ;

Vu le code général des collectivités territoriales ;

Vu la loi organique n° 62-1292 du 6 novembre 1962 modifiée relative à l'élection du président de la République au suffrage universel ;

Vu la loi n° 77-729 du 7 juillet 1977 modifiée relative à l'élection des représentants au Parlement européen ;

Vu la loi n° 88-227 du 11 mars 1988 modifiée relative à la transparence financière de la vie politique ;

Vu la loi n° 2000-493 du 6 juin 2000 tendant à favoriser l'égal accès des femmes et des hommes aux mandats électoraux et fonctions électives ;

Vu le projet de décret présenté par le ministre de l'Intérieur, Après avoir entendu M. Maurice Benassayag en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

Le fichier dénommé « fichier des candidats et des élus », mis en oeuvre par la direction générale de l'administration du ministère de l'Intérieur, a pour finalités d'assurer :

— le suivi des candidatures déposées et des mandats et fonctions exercées par les élus en vue de l'information du Parlement, du gouvernement, de ses délégués et des citoyens ;

— la centralisation des résultats des élections ;

— le contrôle de l'application des législations sur

1) l'interdiction des candidatures multiples ;
2) les cumuls des mandats ;
3) le financement de la vie politique ;
4) l'égal accès des femmes et des hommes aux mandats électoraux et fonc tions électives ;
5) la présentation des candidatures à l'élection présidentielle ;
— l'habilitation des partis et groupements politiques à participer à la campagne en vue d'un référendum, lorsqu'ils sont représentés au sein d'un groupe parlementaire ou en fonction de leurs résultats électoraux.

Sont enregistrés dans le traitement les nom, prénom, sexe, nationalité, date et lieu de naissance, adresse, téléphone des candidats à un mandat électif (à l'exception des candidats aux élections municipales dans les communes de moins de 3 500 habitants) et des personnes élues. S'agissant du scrutin, sont enregistrés le numéro INSEE de la commune, du canton, de la circonscription ou du département, le nombre d'électeurs inscrits, le nombre de votants, le nombre de suffrages exprimés, le nombre de voix obtenues par le candidat, le nombre de sièges à pourvoir et le nombre de sièges obtenus.

Sont en outre enregistrés la nature du mandat électif ou de la fonction élective briguée ou occupée, le sigle et le titre de la liste sur laquelle la personne est candidate ou a été élue ainsi que son rang de présentation, l'étiquette politique choisie par le candidat (ou son remplaçant, le cas échéant), la profession, le nombre de suffrages obtenus, les mandats ou fonctions électives occupés par la personne, les fonctions gouvernementales qu'elle exerce ou a exercé, les distinctions honorifiques dont elle bénéficie ainsi que, pour les parlementaires élus, le groupe de rattachement et le parti de rattachement et, pour les candidats aux élections législatives, le parti de rattachement.

Le ministère envisage enfin d'enregistrer dans le fichier la « **nuance politique** » de chaque candidat qui leur serait attribuée par la préfecture selon une grille des nuances politiques, élaborée pour chaque élection à partir des professions de foi des candidats ou des désistements et fusions opérées entre les deux tours de scrutin. Ce procédé permet au ministère d'additionner, au niveau national, les résultats des élections par famille politique. Toutefois, pour les personnes autres que le maire, élues au conseil municipal dans des communes de moins de 3 500 habitants, aucune information sur l'appartenance politique ne sera enregistrée dans le traitement.

L'enregistrement de cette information, relevant de celles visées par l'article 31 de la loi du 6 janvier 1978, conduit le ministère de l'Intérieur à saisir la Commission d'un projet de décret en Conseil d'État, dont l'article premier alinéa 4 l'autorise à traiter cette donnée. L'exploitation statistique de ces informations doit permettre aux pouvoirs publics et à l'ensemble des citoyens de disposer de résultats d'élections faisant apparaître les tendances politiques dégagées, tant au niveau local que national et revêt, dès lors, un intérêt public.

Dans ces conditions, la Commission estime que les dispositions de l'article premier alinéa 4 du projet de décret, portant application de l'alinéa 3 de l'article 31 de la loi du 6 janvier 1978, ne soulèvent, sur le fond, pas de difficulté. La Commission considère toutefois que les préfets devraient être visés afin d'être autorisés à saisir *ces* informations, dans la mesure où ce sont eux qui, en pratique, déterminent la nuance politique à attribuer à chaque candidat.

Les informations relatives aux candidats non élus seront conservées pendant une durée de deux mois après l'élection (délai du recours contentieux) ; celles relatives aux personnes élues seront conservées pendant la durée de leur mandat. À l'expiration de ces délais, les informations seront versées aux Archives nationales.

Les destinataires des informations traitées seront les membres du gouvernement, les préfets et les services des préfectures chargés de la mise en œuvre des procédures électorales. La Commission relève toutefois que l'article 4 ne mentionne pas le Conseil constitutionnel qui est pourtant habilité à dresser la liste des candidats à l'élection présidentielle au vu des présentations qui lui sont adressées par au moins cinq cents élus (article 3-1 de la loi du 6 novembre 1962 modifiée). À ce titre, il reçoit du ministère de l'Intérieur des informations issues du fichier des élus. La Commission considère en conséquence que l'article 4 du projet de décret doit être modifié en ce sens.

L'article 5 du projet de décret prévoit en outre que toute personne peut, sur simple demande, se voir communiquer les informations relatives à l'identité du candidat ou de l'élu (nom, prénom, sexe, nationalité date et lieu de naissance), à sa profession, ainsi qu'au nombre de suffrages obtenus, à ses mandats ou fonctions électives, à ses fonctions gouvernementales actuelles ou passées ainsi qu'à ses distinctions honorifiques. Le même article prévoit que les organes de presse, les centres de recherche en sciences politiques et les organismes réalisant des sondages pourront obtenir, sur demande, l'ensemble des informations traitées, à l'exclusion de l'adresse et du numéro de téléphone personnels du candidat ou de l'élu.

Or, les informations contenues dans le fichier revêtent la qualité de documents administratifs communicables au sens de la loi du 17 juillet 1978, modifiée par la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec l'administration. Sont en effet communicables à toute personne tous documents administratifs, y compris lorsqu'ils existent sur support informatique. Sont visés, à ce titre, par l'article premier de la loi du 17 juillet 1978 modifiée, les comptes rendus, procès-verbaux et statistiques. Les résultats électoraux constatés par procès-verbal (article R. 67 du code électoral) sont ainsi communicables, après la proclamation des résultats, à toute personne qui en fait la demande (article R. 70 alinéa 2 du code électoral), de même que les informations figurant sur les déclarations de candidature. Lorsque ces résultats sont regroupés au niveau des préfectures et, le cas échéant, cumulés par nuance politique, ils constituent encore un document administratif communicable quel que soit le support ayant permis de les réaliser.

En outre, il résulte de l'article 29 de la loi du 6 janvier 1978, dans sa nouvelle rédaction résultant de la loi du 12 avril 2000, que le titulaire d'un droit d'accès aux documents administratifs exercé conformément aux dispositions de la loi du 17 juillet 1978 ne peut être regardé comme un tiers non autorisé à accéder aux informations. Dès lors, la Commission estime que l'article 5 du projet de décret devrait être supprimé, l'article 4, relatif aux destinataires des informations traitées, pouvant être complété afin de préciser qu'il peut être donné communication à toute personne, sur simple demande, des informations mentionnées au 1er alinéa de l'article 3, à l'exception des informations prévues au b) du même alinéa.

S'agissant du droit d'accès au traitement, il s'exercera directement auprès de la Préfecture du domicile du candidat ou de l'élu, ou auprès de la préfec-

ture de Paris si la personne réside à l'étranger. Au moment du dépôt de candidature, chaque candidat sera informé de l'existence du traitement, des conditions d'exercice de son droit d'accès et de rectification, ainsi que de la grille des nuances politiques retenue pour cette élection et du fait qu'il peut avoir accès au classement qui lui est affecté afin d'en demander, le cas échéant, la rectification soit jusqu'au troisième jour précédant le premier tour d'un scrutin, soit à tout moment après un scrutin. L'article 6 du projet de décret, relatif au droit d'accès, ménage ainsi trois jours pendant lesquels le droit de rectification reconnu par la loi à la personne concernée serait exclu. Cette rédaction vise en réalité à préciser que le délai pour procéder à la rectification demandée serait de trois jours, au minimum. Dès lors, toute demande présentée moins de trois jours avant le scrutin ne pourrait être prise en compte pour la diffusion des résultats. La Commission considère qu'il convient de modifier la rédaction de l'alinéa 2 de l'article 6 du projet de décret.

Émet, au vu de ces observations, un avis conforme au projet de décret présenté par le ministre de l'Intérieur, sous les réserves suivantes :

— que l'article premier, *in fine,* soit rédigé comme suit : « Pour la mise en œuvre de son fichier national des élus et des candidats, et par dérogation aux dispositions de l'article 31 de la loi du 6 janvier 1978 susvisée, le ministre de l'Intérieur et les préfets sont autorisés à collecter, conserver et traiter, dans ce fichier informatisé, des données nominatives faisant apparaître les appartenances politiques des personnes physiques détentrices de l'un des mandats ou de l'une des fonctions énumérées ci-dessus, ou candidates à l'un des scrutins décrits à l'alinéa précédent » ;

— que l'article 4 soit rédigé de la façon suivante : « Le gouvernement et les préfets sont destinataires de l'ensemble des informations collectées et traitées. Le Conseil constitutionnel est également destinataire des informations nominatives nécessaires à l'application de la législation sur la présentation des candidatures à l'élection présidentielle. Il peut être donné communication à toute personne, sur simple demande, des informations mentionnées au 1er alinéa de l'article 3, à l'exception des informations prévues au b) du même alinéa » — que l'article 5 soit supprimé ;

— que l'alinéa 2 de l'article 6 soit rédigé de la façon suivante : « Au moment du dépôt de candidature chaque candidat, ou candidat tête de liste, est informé de la grille des nuances politiques retenue pour l'enregistrement des résultats de l'élection, et du fait qu'il peut avoir accès au classement qui lui est affecté et en demander la rectification, conformément à l'article 36 de la loi du 6 janvier 1978. Toute demande de rectification présentée dans un délai de trois jours précédant le scrutin ne pourra être prise en considération pour la diffusion des résultats ».

Délibération n° 01-021 du 15 mai 2001 relative à une demande d'autorisation présentée par l'Institut de veille sanitaire concernant la constitution d'un système national d'information sur le cancer

(Demande d'autorisation n° 999320)

La Commission nationale de l'informatique et des libertés ;

Saisie pour autorisation du projet de création par l'Institut de veille sanitaire d'un traitement automatisé d'informations indirectement nominatives ayant

pour finalité la constitution d'un système d'information national sur le cancer ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; Vu l'article L. 1413-2 du code de la santé publique ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu l'avis favorable du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé du 16 septembre 1999 ;

Après avoir entendu Monsieur Alain Vidalies, commissaire, en son rapport et Madame Charlotte-Marie pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'Institut de veille sanitaire saisit la Commission nationale de l'informatique et des libertés de la création d'un système d'information national sur le cancer afin de pouvoir disposer de données sur l'état de la situation des cancers en France et de son évolution en termes épidémiologiques tant au plan national, que régional et départemental.

Ce système d'information sera constitué à partir des données de morbidité fournies par les registres de cancer et des données de mortalité transmises par le service commun 8 de l'INSERM chargé de la gestion des causes médicales de décès.

Les registres de cancer qui permettent de recenser dans une zone géographique déterminée les cas de cancer à partir de données nominatives transmises volontairement par les professionnels de santé concernés, communiqueront sur support magnétique à l'Institut de veille sanitaire les informations indirectement nominatives suivantes : un numéro d'enregistrement attribué par chaque registre, le sexe, le mois et l'année de naissance de la personne, le département de résidence, la date de diagnostic, la topographie de la tumeur et sa morphologie.

La Commission prend acte de ce qu'aucune donnée sur l'identité des personnes ne sera communiquée.

Le service commun 8 de l'INSERM chargé, aux termes de l'article L. 2223-42 du code des collectivités territoriales, de l'établissement de la statistique nationale des causes de décès transmettra annuellement par CD-rom à l'Institut de veille sanitaire les données relatives au sexe, à la date de naissance, à la commune et au département du lieu de naissance, à la commune et au département du lieu de domicile, à la cause initiale du décès, à la cause secondaire du décès, à la date du décès et à la commune et au département du lieu de décès.

La Commission estime que les données ainsi transmises sont pertinentes au regard des finalités épidémiologiques poursuivies.

La base nationale ainsi constituée dans les locaux de l'Institut de veille sanitaire sera placée sous la responsabilité d'un médecin nommément désigné qui recevra les données des registres de cancer et de l'INSERM sous pli confidentiel en recommandé. Aucune connexion à Internet ne sera possible à partir de l'ordinateur sur lequel sera implanté le traitement. Des mesures de sécurité physique sont prévues et l'accès logique à l'application sera subordonné, en particulier, à des mots de passe individuels.

La Commission prend acte de ces mesures de sécurité mais estime toutefois souhaitable, au vu de la diversité des missions confiées par le législateur à l'Institut de veille sanitaire et de la multiplicité des applications informatiques appelées à être gérées par l'Institut qu'une évaluation de l'ensemble du système de sécurité soit effectuée. La Commission prend également acte de l'engagement de l'Institut de veille sanitaire à ne pas publier les résultats sous une forme qui permettrait l'identification des individus.

La Commission rappelle qu'aux termes de l'article 40-5 de la loi du 6 janvier 1978 modifiée, toute personne à qui il est proposé de participer à une recherche doit être individuellement informée de la finalité du traitement des données, de la nature des informations transmises, des personnes appelées à être destinataires des données et des modalités pratiques d'exercice du droit d'accès et de rectification.

La loi prévoit, par ailleurs, les cas où il peut être dérogé à cette obligation d'information individuelle lorsque le malade est tenu dans l'ignorance de son pronostic — le médecin traitant n'ayant pas estimé, en conscience, devoir informer son patient de la nature de son mal — ou lorsque les donnés ont été initialement recueillies pour un autre objet que le traitement et qu'il est difficile de retrouver les personnes concernées.

La Commission a considéré, s'agissant des registres de cancer, que les demandes de dérogation à l'obligation d'information individuelle devaient être appréciées au cas par cas par les médecins en charge des patients.

Elle a cependant estimé qu'il incombait aux registres du cancer de diffuser auprès des professionnels de santé participant aux registres une note d'information susceptible d'être remise aux patients qui comporte l'ensemble des points énumérés à l'article 40-5 précité.

La Commission considère qu'il importe que cette note d'information soit complétée afin que le traitement mis en oeuvre par l'Institut de veille sanitaire pour la surveillance nationale du cancer soit mentionné.

Autorise, compte tenu de ces observations, la mise en œuvre par l'Institut de veille sanitaire d'un traitement automatisé d'informations indirectement nominatives ayant pour finalité la constitution d'un système de surveillance national du cancer à partir des données de morbidité transmises par les registres de cancer et des données de mortalité transmises par le service commun 8 de l'INSERM chargé de la gestion des causes médicales de décès.

Recommande, compte tenu des missions imparties par la loi à l'Institut de veille sanitaire et des applications informatiques appelées à être hébergées dans ses locaux de procéder à une évaluation des mesures de sécurité mises en œuvre pour garantir la confidentialité des informations en liaison avec la direction centrale de la sécurité des systèmes d'information.

Délibération n° 01-038 du 12 juin 2001 portant avis sur un projet d'arrêté présenté par le ministre de la Justice portant création d'un traitement relatif à la gestion des procès-verbaux d'infractions de travail illégal destiné à être mis en oeuvre dans les comités opérationnels de lutte contre le travail illégal (COLTI)

(Demande d'avis n° 710332)

La Commission nationale de l'informatique et des libertés ; Saisie par le ministre de la Justice d'un projet d'arrêté portant création d'un traitement automatisé d'informations nominatives à caractère personnel relatif à la gestion des procès-verbaux d'infractions de travail illégal destiné à être mis en œuvre dans tous les comités opérationnels de lutte contre le travail illégal ;

Vu la Convention 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 directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu loi n° 91-1383 du 31 décembre 1991 renforçant la lutte contre le travail clandestin ;

Vu la loi n° 97-210 du 11 mars 1997 relative au renforcement de la lutte contre le travail illégal, pris ensemble le décret n° 97-213 du 11 mars 1997 relatif à la coordination de la lutte contre le travail illégal ;

Vu la délibération de la CNIL n° 99-032 du 27 mai 1999 ;

Vu le projet d'arrêté présenté par le garde des Sceaux, ministre de la Justice ;

Après avoir entendu Monsieur Hubert Bouchet, vice-président délégué, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

La loi du 31 décembre 1991 relative à la lutte contre le travail clandestin a inséré dans le code du travail les articles L. 324-9 et suivants qui instituent un dispositif destiné à lutter contre le travail illégal et prévoient une coordination entre les différents corps de contrôle.

Par ailleurs, la loi du 11 mars 1997 a inséré dans le code du travail un article L. 324-13-2 qui prévoit que les aides publiques à l'emploi ou à la formation professionnelle peuvent être refusées aux personnes physiques ou morales ayant fait l'objet d'un procès-verbal constatant l'existence d'une infraction de travail dissimulé ou de marchandage.

Le décret du 11 mars 1997 relatif à la coordination de la lutte contre le travail illégal a créé plusieurs instances ayant pour mission de favoriser la lutte contre le travail dissimulé, l'emploi non déclaré, l'introduction et l'emploi illicites de main-d'œuvre étrangère, le marchandage, le prêt illicite de main - d'œuvre, le cumul a emplois, le placement et le cumul irrégulier de revenus de remplacement avec les revenus d'un emploi.

À cet effet, ont été créés dans chaque département des comités opérationnels de lutte contre le travail illégal (COLTI) qui ont pour mission de coordonner les opérations de contrôle, de recenser les moyens nécessaires à ces opérations, de mettre à disposition des URSSAF et des services des impôts les informations nécessaires au recouvrement des cotisations sociales et des impôts, de. veiller aux échanges d'informations en direction des services de protection sociale en application de l'article L. 324-13 du code du travail et d'établir des statistiques destinées à mieux appréhender le phénomène du travail illégal.

Le projet d'arrêté soumis à l'examen de la Commission a pour objet de créer, au sein de chaque COLTI, dans tous les départements, un traitement automatisé d'informations nominatives de centralisation et de suivi des procès-verbaux établis en matière de travail illégal en vue d'échanger ces informations entre les différents agents chargés du contrôle et des suites administratives ou judiciaires. Ce traitement a pour finalités de mettre à disposition des services chargés d'opérer des recouvrements des informations concernant les procédures engagées contre une personne physique ou morale et leurs résultats en matière pénale ou administrative, de permettre aux services enquêteurs, préalablement à une intervention programmée à l'encontre d'une personne, de vérifier si la personne concernée fait ou a déjà fait l'objet d'une procédure en matière de lutte contre le travail illégal, de permettre au parquet de déclencher certaines enquêtes, et aux autorités concernées de mettre en œuvre les dispositions de l'article L. 324-13-2 du code du travail, enfin, d'effectuer un suivi statistique de l'action des services enquêteurs et des réponses judiciaires et administratives ainsi qu'un suivi de la jurisprudence. L'article 30 de la loi du 6 janvier 1978 réservant aux seules juridictions et autorités publiques agissant dans le cadre de leurs attributions légales le traitement automatisé d'informations nominatives concernant les infractions et condamnations, il y a lieu d'observer que les COLTI, placés sous l'autorité du procureur de la République territorialement compétent, sont habilités, eu égard aux dispositions législatives et réglementaires citées ci-dessus, à procéder à un traitement de cette nature.

Seront enregistrés dans le traitement les nom, prénom, date de naissance, nationalité, sexe, qualité et qualification du mis en cause, la qualité de l'emploi salarié objet de la plainte, les numéro de procédure, de parquet et qualité du service enquêteur, la date des faits, la date de clôture du procès-verbal, le mode de saisine, des informations sur le contrôle (lieu, coordination), les nom, adresse, numéro SIRET et forme juridique de la société, la relation économique, la nationalité si l'entreprise est étrangère, l'adresse du lieu du constat, le type de lieu, le secteur d'activités concerné, le nombre de salariés et le nombre de salariés illicites, la nature de l'infraction constatée et le nombre d'infractions, ainsi que la nature des suites judiciaires apportées à l'affaire, les condamnations prononcées dans la procédure visée, la date du jugement, la mention d'un éventuel appel ou pourvoi en cassation et les éventuelles suites fiscales, sociales ou relatives aux aides publiques.

La Commission prend acte qu'aucune information nominative relative aux salariés ne sera enregistrée dans le traitement.

Le projet d'arrêté prévoit que les informations seront conservées pendant une durée de cinq ans à compter de leur inscription. Cette durée de conservation est pertinente et adaptée aux dispositions de l'article 324-13-2 du code du travail qui prévoit que les aides publiques à l'emploi ou à la forma-

tion professionnelle peuvent être refusées pendant une durée maximale de cinq ans aux personnes physiques ou morales ayant fait l'objet d'un procès-verbal pour travail dissimulé ou marchandage.

Le projet d'arrêté prévoit en outre que, en cas de non-lieu ou de relaxe, les informations nominatives relatives aux dirigeants et aux entreprises seront effacées dans un délai de dix jours à compter de la date à laquelle la décision est devenue définitive. En cas de classement sans suite, les informations seront effacées dans un délai de dix jours à compter de la date de la décision de classement.

La Commission relève que l'article 4 du projet d'arrêté précise que sont habilités à obtenir communication des informations traitées les magistrats du ou des parquets du ressort du COLTI, les membres du COLTI, ainsi que les agents habilités, aux termes de l'article L. 324-12 du code du travail, à constater les infractions en matière de travail dissimulé. Toutefois, seul le secrétaire permanent du COLTI, placé sous l'autorité du procureur de la République, disposant d'un accès direct au fichier, la rédaction de cet article devrait être précisée afin de distinguer, d'une part, les personnes et autorités disposant d'un accès direct au fichier (le procureur de la République et le secrétaire permanent du COLTI), d'autre part, les autres autorités et organismes qui pourront être destinataires des informations sur demande. Enfin, la Commission prend acte que les services de la délégation interministérielle à la lutte contre le travail illégal (DILTI) seront uniquement destinataires d'informations concernant des personnes morales.

Le droit d'accès et de rectification aux informations traitées s'exercera auprès du secrétariat permanent des COLTI. Les personnes en seront informées lors de l'établissement des procès-verbaux.

Émet un avis favorable au projet d'arrêté présenté par le garde des Sceaux, ministre de la Justice, sous réserve que l'article 4 du projet d'arrêté soit ainsi rédigé :

« Disposent seuls d'un accès direct au traitement les magistrats du ou des parquets du ressort et le secrétaire permanent du COLTI, placé sous l'autorité du procureur de la République.

Peuvent en outre être destinataires des informations enregistrées dans le traitement les membres du COLTI ainsi que, sur leur demande, [les autres catégories d'agents ou de fonctionnaires visés par l'article 4 du projet d'arrêté].»

Délibération n° 01 -044 du 4 septembre 2001 portant avis sur un projet de décret en Conseil d'État relatif à l'utilisation du RNIPP et sur un projet d'arrêté interministériel concernant la réalisation d'un échantillon inter-régimes d'allocataires de minima sociaux par la direction de la recherche, des études, de l'évaluation et des statistiques du ministère de l'Emploi et de la Solidarité

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis d'un projet de décret en Conseil d'État relatif à l'utilisation du répertoire national d'identification des personnes physiques pour la mise en œuvre d'un échantillon national inter-régimes d'allocataires de minima

sociaux, et d'un projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie, de la ministre de l'Emploi et de la Solidarité, et du ministre de l'Agriculture et de la Pêche relatif à des traitements de données à caractère personnel pour la mise en œuvre de l'échantillon national interrégimes d'allocataires de minima sociaux (demande d'avis n° 759541) ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 pris pour son application ;

Vu la loi n° 98-657 du 29 juillet 1998 d'orientation relative à la lutte contre les exclusions ;

Après avoir entendu Monsieur Pierre Schapira, commissaire en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Sur les finalités poursuivies

La Commission nationale de l'informatique et des libertés est saisie par la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) du ministère de l'Emploi et de la Solidarité d'une demande d'avis concernant la constitution d'un échantillon national inter-régimes d'allocataires de minima sociaux afin de permettre aux pouvoirs publics de mieux connaître les « trajectoires » des personnes bénéficiaires de certains minima sociaux (revenu minimum d'insertion, allocation d'adulte handicapé, allocation de parent isolé, allocation de solidarité spécifique) entre les dispositifs à vocation sociale relevant de la Caisse nationale des allocations familiales (CNAF) ou de la Caisse centrale de la mutualité sociale agricole (CCMSA) et ceux relevant de l'indemnisation du chômage (UNÉDIC).

L'échantillon national inter-régimes d'allocataires de minima sociaux devra permettre à la DREES de produire régulièrement des informations statistiques sur l'évolution de la situation des allocataires des minima sociaux et leur passage éventuel par des situations de chômage.

Sur la base d'une convention définissant la finalité de l'étude et contenant l'engagement des organismes destinataires à ne pas utiliser les données à d'autres fins et à en assurer la confidentialité, l'échantillon pourra être ponctuellement mis à disposition des partenaires du dispositif (INSEE, CCMSA, CNAF, UNÉDIC), des services statistiques ou d'études ministériels et d'organismes d'études.

La Commission estime qu'elle doit être saisie pour avis du modèle de convention de cession.

Par ailleurs, l'échantillon national pourra servir de base de sondage pour la réalisation, au bénéfice de la DREES, d'enquêtes statistiques nécessitant une

prise de contact avec les allocataires concernés pour affiner l'analyse découlant des seuls indicateurs présents dans l'échantillon.

Enfin, les organismes sociaux partenaires pourront mettre en œuvre, à l'occasion de la constitution de l'échantillon national, des bases de sondage pour leurs besoins propres en termes d'enquêtes auprès de leurs allocataires.

Dans tous les cas, la Commission prend acte de ce que la réalisation d'enquêtes auprès des personnes composant l'échantillon national à partir des bases de sondage constituées ne se fera qu'après avis de la CNIL et considère qu'il convient d'en faire mention aux articles 1 et 6 du projet d'arrêté.

La Commission estime que les finalités ainsi poursuivies, qui s'inscrivent dans le prolongement des politiques publiques dans le domaine social telles que définies par la loi d'orientation relative à la lutte contre les exclusions, sont légitimes.

Sur *les modalités de transmission et de traitement des informations*

La mise en oeuvre de l'échantillon national sera réalisée en trois étapes.

La première étape reposera sur la constitution, par l'INSEE, d'un « fichier d'identification de l'échantillon » concernant les personnes nées entre le 1er et le 14 du mois d'octobre et âgées de plus de 16 ans et de moins de 65 ans à la date de l'extraction. Pour chacune des personnes concernées, ce fichier comprendra, d'une part, des informations extraites du répertoire national d'identification des personnes physiques (numéro d'inscription au répertoire-NIR, nom patronymique, prénoms, sexe, date et lieu de naissance) et, d'autre part, un numéro d'ordre personnel propre à l'échantillon national inter-régimes d'allocataires des minirna sociaux qui est attribué par l'INSEE à chaque membre du fichier.

L'INSEE transmettra ce fichier à la CCMSA, à la CNAF et à l'UNÉDIC.

La deuxième étape consistera en l'extraction, par les trois organismes sociaux, des données relatives aux allocataires concernés à partir de leurs fichiers de gestion. Ces données seront ensuite appariées à l'aide du NIR avec celles du « fichier d'identification de l'échantillon » pour comporter les informations suivantes au niveau de la CCMSA et de la CNAF : numéro d'inscription au répertoire (NIR), numéro d'ordre personnel propre à l'échantillon, numéro d'ordre dans l'organisme de base, nom patronymique, prénoms, sexe, date et lieu de naissance, état matrimonial, nationalité, code commune INSEE de résidence, situation familiale, activités, revenus, prestations légales perçues. Le fichier constitué par l'UNEDIC intégrera également des données sur le diplôme, le type d'allocation perçue, les caractéristiques de la prise en charge, les caractéristiques du dernier contrat de travail et l'existence d'une formation suivie ou d'une activité réduite.

La CCMSA, la CNAF et l'UNÉDIC transmettront ensuite à la DREES les données contenues dans les fichiers ainsi constitués.

La Commission prend acte de ce que le NIR ne sera utilisé que pour apparier les données sélectionnées contenues dans les fichiers de gestion des organismes sociaux, et que ni ce numéro, ni le numéro d'ordre dans l'organisme de base, ni l'identité des personnes, pas plus que leur jour de naissance ne figureront au sein des fichiers transmis à la DREES.

La troisième étape consistera en l'appariement, par la DREES, des fichiers transmis par les trois organismes sociaux grâce aux seuls numéros d'ordre personnels propres à l'échantillon, pour permettre la création de l'échantillon national d'allocataires de minima sociaux. Ces numéros d'ordre personnels constitueront la seule information susceptible de permettre à la fois le chaînage des données dans le temps et la constitution, par la DREES, de bases de sondage pour la réalisation d'enquêtes auprès des personnes composant l'échantillon.

En cas de transmission — prévue par convention — d'une copie de l'échantillon à des services statistiques ou d'études ministériels ou à des organismes d'études, la DREES « anonymisera » la base de données en remplaçant les numéros d'ordre personnels de l'échantillon par de nouveaux numéros d'ordre.

La Commission estime que les modalités de transmission de ces données garantissent de façon satisfaisante leur confidentialité.

Sur la nature des informations traitées

L'échantillon comportera des variables descriptives de la situation des allocataires — qui concernent la situation familiale et financière de l'allocataire, les caractéristiques de sa prise en charge et les types de prestations perçues — et en particulier leur nationalité (sous la forme « Français, CEE, autre ») et leur lieu de naissance.

Ces données permettent de mieux comprendre les trajectoires socio-professionnelles et les éventuelles difficultés d'insertion que peuvent rencontrer les allocataires de minima sociaux.

La Commission relève cependant que le recueil, au sein des fichiers de gestion des organismes sociaux partenaires, de l'identité à la fois de l'allocataire et de son conjoint est dénué de pertinence et demande en conséquence de substituer, au sein de l'article 4 du projet d'arrêté, « nom patronymique » à l'intitulé « nom patronymique de l'allocataire et de son conjoint ».

Sous cette réserve, la Commission considère que les informations utilisées dans le cadre de l'échantillon national de bénéficiaires de minima sociaux sont pertinentes, adéquates et non excessives au regard des finalités poursuivies.

Sur le droit d'opposition des personnes concernées par l'échantillon

La Commission estime que le droit d'opposition à figurer dans l'échantillon ne doit pas être écarté dans la mesure où ce traitement statistique ne revêt aucun caractère obligatoire et demande, en conséquence, la suppression de l'article 11 du projet d'arrêté.

Sur l'information et le droit d'accès des personnes concernées par le traitement

La Commission prend acte de l'engagement de la DREES à ce que l'ensemble des organismes sociaux partenaires de l'échantillon procède à une information à caractère général sur la mise en œuvre de l'échantillon, notamment par l'insertion d'encarts dans les publications de ces organismes.

Le droit d'accès s'exercera auprès de l'INSEE, de la CCMSA, de la CNAF, de l'UNEDIC et de la DREES pour les fichiers qu'ils détiennent dans le cadre de la mise en œuvre de l'échantillon.

Compte tenu de ces observations, la Commission :
émet un avis favorable au projet de décret en Conseil d'État présen té en application de l'article 18 de la loi du 6 janvier 1978 ;
émet un avis favorable au projet d'arrêté interministériel présenté en application de l'article 15 de la loi du 6 janvier 1978, **sous la réserve** qu'il soit fait mention aux articles 1 et 6 du fait que les enquêtes ne seront mi ses en œuvre qu'après avis de la CNIL, qu'au sein de l'article 4 l'expression « noms patronymiques de l'allocataire et de son conjoint » soit remplacée par celle de « nom patronymique » et que l'article 11 soit supprimé ;
demande à être saisie du modèle de convention de cession de l'échan tillon national inter-régimes d'allocataires de minima sociaux mis en place par la DREES.

Délibération n° 01 -046 du 18 septembre 2001 portant avis sur un traitement automatisé de constitution des listes électorales prud'homales en vue du scrutin du 11 décembre 2002

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis du projet d'arrêté relatif à un traitement automatisé de constitution des listes électorales prud'homales en vue du scrutin du 11 décembre 2002 présenté par le ministère de l'Emploi et de la Solidarité ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu la loi du 3 janvier l979, modifiée, sur les archives ; Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le code du travail et notamment les dispositions du titre 1er du Livre V ;

Vu la délibération n° 91-104 du 5 novembre 1991 portant avis sur le projet d'arrêté et sur les projets de décret présentés par le ministre du Travail, de l'Emploi et de la Formation professionnelle concernant un projet d'automatisation des listes électorales prud'homales ;

Vu la délibération n° 96-071 du 1er octobre 1996 portant avis sur le projet d'arrêté présenté par le ministère du Travail et des Affaires sociales concernant la constitution automatisée des listes électorales en vue du scrutin prud'homal du 10 décembre 1997 ;

Vu la délibération n° 96-072 du 1er octobre 1996 portant recommandation concernant les traitements automatisés d'informations nominatives relatifs à la gestion par les mairies, du fichier électoral prud'homal ;

Après avoir entendu Monsieur Hubert Bouchet, vice président délégué, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Les élections prud'homales permettent à 15 millions de salariés et d'employeurs d'élire leurs 14 646 conseillers prud'homaux. La principale caractéristique de cette justice est de fonctionner de façon paritaire avec des juges non professionnels élus par leurs justiciables.

Les conseils de prud'hommes sont organisés en sections : industrie, commerce, agriculture, activités diverses et encadrement, chaque section divisée en deux collèges employeurs et salariés. Chaque électeur doit voter dans son collège et dans sa section, déterminés par le type d'emploi et par le type d'employeur.

Les élections prud'homales se déroulent tous les cinq ans, et lors de chaque scrutin il est nécessaire de procéder à l'établissement de la liste électorale, mission incombant au ministère de l'Emploi et de la Solidarité avec le concours de nombreux acteurs. **1**) **Les informations utilisées**

Les informations concernant les employeurs relevant du régime général de sécurité sociale et leurs salariés seront transmises par la CNAVTS. Il s'agit du numéro SIRET, du code NIC du siège social, de la date de création de l'établissement de la raison sociale, de l'enseigne de l'établissement, de l'adresse de localisation géographique, de l'adresse de correspondance, du code indiquant le mode papier ou magnétique de la déclaration DADS, de l'effectif total de l'établissement et du code APE.

Les informations concernant les employeurs relevant du régime agricole et leurs salariés seront communiquées par la MSA. Il s'agit de l'identifiant (SIRET et MSA), du code département de la caisse MSA gérant l'établissement, du nom ou de la raison sociale, de l'adresse, du code indiquant le mode de déclaration trimestrielle, de l'effectif total de l'établissement et du code APE de l'établissement.

Les informations concernant les employeurs relevant des régimes spéciaux et leurs salariés (EDF-GDF, RATP, SNCF, CANSSM, clerc et employés de notaires) seront l'identifiant, (SIRET), le nom ou la raison sociale, l'adresse, l'effectif total de l'établissement et le code APE.

L'UNEDIC transmettra les informations relatives aux salariés involontairement privés d'emploi.

S'agissant des salariés, conformément aux dispositions de l'article R. 513-11 du code du travail (décret du 12 mars 1992) les informations collectées et traitées seront : l'identification de l'employeur, les noms et prénoms, les dates et lieux de naissance, les adresses et le NIR.

Le NIR, identifiant commun à tous les salariés, est utilisé dans le cadre de la constitution des listes électorales prud'homales, pour permettre au prestataire de service informatique du ministère du Travail de détecter les multi inscriptions. Toutefois, les listes communiquées aux mairies ou aux préfectures ne comportent pas ce numéro. La délibération 91-104 du 5 novembre 1991 avait émis un avis favorable du projet de décret, de portée générale et permanente, énumérant les informations transmises par les employeurs sur les salariés et comprenant le NIR.

L'utilisation dans des conditions strictement identiques du NIR pour le scrutin de 2002 ne soulève pas de difficultés.

2) Les destinataires des informations

Les mairies destinataires des listes électorales provisoires, des listes de rejet et des listes de multi-inscrits, sont gestionnaires des listes électorales et des cartes d'électeurs. Elles devront se conformer aux dispositions de la recommandation concernant les traitements automatisés d'informations nominatives relatives à la gestion par les mairies, du fichier électoral prud'homal du 1er octobre 1996.

3) L'information des électeurs

Outre la publication de l'arrêté du ministère de l'Emploi et de la Solidarité es au Journal officiel il sera fait mention de l'article 27 sur les différents imprimés envoyés aux déclarants pour effectuer leurs déclarations.

Il appartient également aux employeurs d'informer leurs salariés de la possibilité d'exercer leur droit d'accès et de rectification auprès du ministère du Travail. L'information des électeurs sera faite, notamment, par l'affichage dans les entreprises pendant quinze jours des listes électorales. Les salariés involontairement privés d'emplois seront informés par l'envoi de la déclaration qui leur est adressée par l'UNEDIC. Sur ces documents figureront les mentions de l'article 27 de la loi du 6 janvier 1978.

Ce droit d'accès et de rectification pourra être exercé à partir de juin 2002 (date de réception par les mairies des listes provisoires) jusqu'à l'expiration des délais de recours contentieux soit le 10 avril 2003.

5) La conservation des données et transmission aux Archives nationales

À l'issue du scrutin, tous les supports de saisie seront détruits ainsi que les listes électorales et documents intermédiaires détenus par les mairies.

Le ministère conservera pendant une année après le scrutin une copie du fichier électoral, en cas d'élections complémentaires. Cette copie sera détruite au plus tard le 11 décembre 2003.

Le ministère conservera également une copie du fichier des établissements ainsi qu'un fichier statistique sur l'électorat constitué à l'issue des élections, sans que ces fichiers ne comportent d'information nominative.

Le ministère conservera une copie de la liste électorale, avec dénaturation des identités des électeurs afin de l'utiliser comme test dans la perspective de la préparation du scrutin de 2007.

Ces deux fichiers seront conservés jusqu'en décembre 2006, soit un an avant la date des prochaines élections, date à laquelle ils seront détruits.

Les fichiers constitutifs de la liste électorale dans leur état définitif seront versés aux Archives nationales à l'issue des scrutins de 2002 ainsi qu'un fichier comportant le premier caractère du NIR (sexe) des électeurs.

Le ministère dispose d'un délai d'utilité administrative de quatre ans à partir de la date de versement des fichiers aux Archives nationales (du 11 avril 2003 au 11 avril 2007).
Le ministère devra communiquer à la CNIL le descriptif des données versées aux Archives nationales et associer la Commission aux opérations de transferts des données aux Archives nationales.

Au bénéfice de ces observations :

Émet un avis favorable au projet d'arrêté portant création d'un traitement automatisé de constitution des listes électorales prud'homales en vue du scrutin du 11 décembre 2002.

Délibération n° 01-047 du 18 septembre 2001 portant avis sur un traitement sur les fichiers des électeurs inscrits sur les listes électorales prud'homales de 1997, versées aux Archives nationales, à des fins statistiques et d'études présenté par le ministère de l'Emploi et de la Solidarité

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis du projet d'arrêté relatif à un traitement sur les fichiers des électeurs inscrits sur les listes électorales prud'homales de 1997, versées aux Archives nationales, à des fins statistiques et d'études présentées par le ministère de l'Emploi et de la Solidarité ;

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

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu la loi du 3 janvier 1979, modifiée, sur les archives ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le code du travail et notamment les dispositions du titre 1er du Livre V ;

Après avoir entendu Monsieur Hubert Bouchet, vice président délégué, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère de l'Emploi et de la Solidarité a déposé une demande d'avis relative à un traitement sur les fichiers des électeurs inscrits sur les listes électorales prud'homales de 1997, versées aux Archives nationales, à des fins statistiques et d'études.

Le ministère de l'Emploi et de la Solidarité souhaite pouvoir accéder aux listes électorales établies pour le scrutin de 1997 afin de constituer un fichier des entreprises multi-établissements et afin de répondre aux exigences de l'article 12 de la loi du 9 mai 2001 (article L. 513-6 du code du travail) relative à l'égalité professionnelle entre les femmes et les hommes. Cet article précise que « pour le prochain renouvellement des conseils de prud'hommes, les organisations présentant des listes de candidats devront faire en sorte de présenter une proportion de femmes et d'hommes réduisant d'un tiers, par rapport au précédent scrutin, l'écart entre la représentation du sexe sous-représenté au sein des listes et sa part dans le corps électoral selon des modalités propres à favoriser la progression du pourcentage de femmes élues. [...] ».

L'exploitation des fichiers de 1997 permettrait de disposer d'une base de référence des entreprises comportant plusieurs établissements permettant de fiabiliser le processus d'élaboration de la liste électorale et là même de limiter les erreurs d'inscription et donc les recours contentieux.

Les informations qui sont conservées pour ce fichier multi-établissement sont le code origine de la déclaration, le code département, le type d'employeur, l'identification de l'employeur, la raison sociale et le code INSEE de la commune de la liste provisoire, le code INSEE de la commune de vote, le code INSEE de la commune cédante, l'effectif.

Par ailleurs, les informations qui seraient conservées afin de connaître le nombre d'électeur de chaque sexe dans chaque collège et section pour établir leur part respective et le nombre d'élus par sexe pour chaque section et collège de façon à indiquer aux organisations syndicales présentant des candidats le nombre d'hommes et de femmes à inscrire sur leurs listes, sont : le lieu de vote, le premier chiffre du NIR, le collège et la section et le code INSEE de la commune de vote.

Les deux premiers caractères du nom d'épouse et le prénom ne seront extraits du fichier électoral de 1997 que lorsque le NIR ne sera pas exploitable (NIR tronqué ou inexistant).

Ces deux fichiers ne comportent pas après traitement, de données nominatives et présentent un intérêt certain.

Le sous traitant informatique du ministère de l'Emploi procédera dans les locaux des Archives nationales, sous la surveillance et le contrôle du personnel des Archives nationales, au traitement d'extraction des données concernées.

Au bénéfice de ces observations :

Emet un avis favorable au projet d'arrêté portant création d'un traitement sur les fichiers des électeurs inscrits sur les listes électorales de 1997, versés aux Archives nationales, à des fins statistiques et d'études présentées par le ministère de l'Emploi et de la Solidarité.

Sous réserve que l'article 2 4e tiret du projet d'arrêté soit rédigé sous la forme :

« un fichier d'analyse statistique de représentation des femmes dans l'électorat prud'homal de 1997 comportant le premier caractère du numéro d'inscription au RNIPP ou à défaut le prénom et les deux premiers caractères du nom d'épouse, le collège, la section et le lieu de vote. »

Délibération n° 01-048 du 18 septembre 2001 relative au projet de décision du comité des établissements de crédit et des entreprises d'investissement portant création d'un fichier des dirigeants et actionnaires des établissements de crédit et des entreprises d'investissement dénommé « FIDEC »

(Demande d'avis n° 733724)

La Commission nationale de l'informatique et des libertés ; Saisie par le Comité des établissements de crédit et des entreprises d'investissement (CECEI) d'une demande d'avis relative à la mise en œuvre d'un traitement automatisé de données nominatives dénommé « FIDEC » ayant pour finalité la centralisation d'informations susceptibles de permettre d'ap-

précier l'expérience, la compétence et l'honorabilité des dirigeants et actionnaires personnes physiques des établissements de crédit et des entreprises d'investissement ;

Vu la Convention du 28 janvier 1981 du Conseil de l'Europe 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 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le code monétaire et financier, notamment ses articles L. 511-9 à L. 511-20, L. 532-1 à L. 532-10 à L. 532-13, L. 612-1 à L. 612-7 et L 631-1 à L. 632-1 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 précitée ;

Vu le projet de décision du président du Comité des établissements de crédit et des entreprises d'investissement ;

Après avoir entendu Monsieur Pierre Leclercq, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

Le Comité des établissements de crédit et des entreprises d'investissement (CECEI) a saisi la Commission d'une demande d'avis relative à la mise en œuvre d'un traitement automatisé de données nominatives dénommé « FIDEC » ayant pour finalité la centralisation d'informations susceptibles de permettre d'apprécier l'expérience, la compétence et l'honorabilité des dirigeants et actionnaires personnes physiques des établissements de crédit et des entreprises d'investissement ;

Le CECEI est chargé de délivrer l'agrément que les établissements de crédit et entreprises d'investissement doivent obtenir, conformément aux dispositions de l'article L. 532-1 du code monétaire et financier, pour pouvoir exercer leurs activités.

À cette fin, il vérifie, aux termes mêmes de l'article L. 511 -10 du code monétaire et financier, que les dirigeants des établissements de crédit possèdent à tout moment l'honorabilité et la compétence nécessaires, ainsi que l'expérience adéquate à leurs fonctions.

Dans le cadre de sa mission de surveillance et de contrôle, le CECEI est amené à collaborer avec la Commission bancaire (CB), s'agissant du respect, par les prestataires de services d'investissement des dispositions législatives et réglementaires qui leur sont applicables (article L. 613-1 du code monétaire et financier), avec la Commission des opérations de bourse (COB), s'agissant des services de gestion de portefeuille (article L. 621 -22 du même code), et avec le Conseil des marchés financiers (CMF), s'agissanf des conditions d'exercice, par les prestataires de services d'investissement, de leur activité (article L. 622-7).

En outre, le CECEI est l'interlocuteur unique des entreprises demanderesses : il reçoit les dossiers de demande d'agrément et leur réclame, le cas échéant, les compléments d'information nécessaires avant de les transmettre aux autres autorités compétentes. C'est à ce titre de « guichet unique » qu'il procède à la déclaration du traitement projeté.

Le traitement envisagé recensera les informations nominatives suivantes : l'état civil (noms patronymique et usuel, prénoms, sexe, date et lieu de naissance, nationalité, adresse personnelle, nom et prénoms des parents), le *curriculum vitae* (expérience professionnelle et, éventuellement, diplômes), les références du questionnaire rempli à l'appui de la demande d'agrément (références, date, existence éventuelle d'informations significatives), références des dossiers d'instruction de candidatures formulées antérieurement auprès du CECEI, existence de sanctions ou décisions défavorables non amnistiées et notifiées à l'intéressé émanant du CECEI, de la CB, du CMF, de la COB ou du CDGF, constatation d'une transmission de renseignement inexacts auprès de l'une de ces cinq autorités, mention d'un retrait de candidature auprès du CECEI, du CMF ou de la COB, références de procès-verbaux mettant fin aux fonctions d'un dirigeant, retrait d'agrément d'office ou initié par le CECEI, le CMF ou la COB, mention des ordres donnés par la CB de procéder à des publications rectificatives de comptes présentant des inexactitudes ou des omissions, mention d'avis défavorable par la CB à la désignation d'un commissaire aux comptes, références des documents dont une des cinq autorités a prévu l'inscription dans la base.

Ces informations apparaissent pertinentes au regard de la finalité du traitement.

S'agissant des données collectées directement auprès des personnes, les intéressés sont informés, par le questionnaire de demande d'agrément, du fondement juridique de la collecte, du caractère obligatoire des réponses à fournir, des organismes destinataires (CECEI, CB, Banque de France, CMF et COB), de la possibilité d'exercer leur droit d'accès et de rectification auprès de la direction des établissements de crédit et des entreprises d'investissement de la Banque de France, ainsi que du délai et de la forme de la réponse à leur demande de droit d'accès.

Sur ce point, la Commission rappelle que si, pour des raisons pratiques, le droit d'accès au fichier du CECEI peut s'exercer dans les locaux de la Banque de France, regardée comme sous-traitant, c'est à la condition expresse que cette consultation soit effectuée sous la responsabilité du président du CECEI, organisme déclarant et responsable juridique du traitement au sens de la loi du 6 janvier 1978.

S'agissant des informations collectées indirectement, celles-ci ne seront enregistrées qu'après avoir été notifiées aux intéressés ou après qu'ils auront été mis en mesure de présenter des observations écrites.

Le CECEI a souhaité exclure, en application de l'article 26 de la loi, la possibilité pour les intéressés de s'opposer à ce que des informations nominatives les concernant soient saisies et traitées dans le fichier projeté. Cette demande paraît pertinente compte tenu de la finalité poursuivie.

La base FIDEC sera interconnectée avec la base de données des agents financiers (BAFI), déclarée par la Banque de France le 16 octobre 1991 et ayant fait l'objet d'un avis favorable de la CNIL en date du 8 avril 1992.

En outre, afin de connaître la cotation des entreprises concernées et de leurs dirigeants, l'inscription dans la base FIDEC donnera lieu à une consultation automatique du fichier bancaire des entreprises (FIBEN), déclaré le 27 février 1981 auprès de la Commission et qui a fait l'objet de plusieurs modifications depuis l'avis favorable rendu le 7 juillet 1987.

La durée de conservation des informations nominatives traitées est soit de 20 ans, s'agissant de l'état civil et du *curriculum vitae* des intéressés, soit de 15 ans pour ce qui concerne les autres informations collectées. Dans la mesure où l'objet même de la base projetée est d'empêcher des dirigeants ou des actionnaires d'établissements de crédit ou d'entreprises d'investissement qui se seraient signalés négativement de pouvoir diriger à nouveau une société de ce type, cette durée n'apparaît pas excessive.

Afin de pouvoir disposer de l'ensemble des éléments et documents lui permettant d'apprécier l'honorabilité des dirigeants et la qualité des actionnaires des établissements de crédit et des entreprises d'investissement, le CECEI a souhaité obtenir communication du bulletin n° 2 du casier judiciaire, comme d'ailleurs la CB, la COB et le CMF.

Le contenu du casier ne sera pas stocké dans FIDEC et seule la réponse électronique du casier y figurera sous la forme « casier vierge », « réponse par courrier » ou « erreur dans la demande ». Cette réponse sera conservée deux mois dans la base.

Sur ce point, la Commission demande dans un souci de clarté que les formules « casier vierge » et « réponse par courrier » soient remplacées par « néant au bulletin n° 2 » et « inscription au bulletin n° 2 ».

S'agissant de la conservation des bulletins sur support papier, la Commission demande que le CECEI s'engage à interroger le casier judiciaire lors de l'examen de chaque demande d'agrément et qu'un bulletin du casier judiciaire demandé par le passé ne puisse être utilisé dans l'instruction d'une demande nouvelle.

Plusieurs autorités (CB, CMF, CDGF et COB) ont vocation, à raison de leurs responsabilités, à avoir accès à ce traitement. Cette possibilité de communication trouve son fondement juridique dans les dispositions de l'article L. 631-1 du code monétaire et financier.

L'organisme déclarant (CECEI) et les différents destinataires mentionnés dans le projet de décision portant création du traitement (CB, CMF, COB et CDGF) sont tenus au secret professionnel en vertu des dispositions du même code.

Le fonds de garantie des dépôts, institué par l'article L. 312-4 du code monétaire et financier, ainsi que les autorités étrangères, figurent au nombre des destinataires des informations de la base FIDEC, mais n'auront pas un accès direct, sous forme électronique, au traitement. Il appartiendra à leur personnel, pour l'exercice de leurs missions, de s'adresser au CECEI ou à l'une des quatre autorités ayant accès au traitement.

La transmission, par le CECEI, d'informations à des autorités de surveillance étrangères trouve son fondement dans l'article L. 612-6 du code monétaire et financier et n'est possible qu'à la condition, notamment, que cette possibilité de communication soit réciproque et que le personnel de ces autorités soient soumis au secret professionnel.

Émet, au bénéfice de ces observations, un avis favorable au projet de décision du président du CECEI portant création de la base « FIDEC ».

Délibération n° 01-049 du 18 septembre 2001 relative au projet de décret du Premier ministre modifiant l'article R. 79 du code de procédure pénale relatif au casier judiciaire

La Commission nationale de l'informatique et des libertés ;

Saisie par la présidente de la Commission de l'informatique, des réseaux et de la communication électronique du ministère de la Justice d'un projet de décret du Premier ministre modifiant l'article R. 79 du code de procédure pénale tendant à permettre au Comité des établissements de crédit et des entreprises d'investissement, à la Commission des opérations de bourse, au Conseil des marchés financiers et à la Commission bancaire d'avoir accès au bulletin n° 2 du casier judiciaire ;

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

Vu le code de procédure pénale, et notamment ses articles 776, 779 et R. 79;

Vu le code monétaire et financier ;

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

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 précitée ;

Vu le projet de décret du Premier ministre ;

Après avoir entendu Monsieur Pierre Leclercq, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

Les dirigeants d'établissements de crédit et d'entreprises d'investissement, du fait de leurs responsabilités spécifiques, font l'objet d'une surveillance imposée par la loi de la part d'autorités spécialisées.

À ce titre, lors de l'examen des demandes d'agrément nécessaire à l'exercice des activités de ces établissements, le Comité des établissements de crédit et des entreprises d'investissement (CECEI) vérifie, en application de l'article L. 511-10 du code monétaire et financier, que les dirigeants des établissements de crédit possèdent à tout moment l'honorabilité et la compétence nécessaires, ainsi que l'expérience adéquate à leurs fonctions.

À cette fin, le CECEI, ainsi que la Commission des opérations de bourse, le Conseil des marchés financiers et la Commission bancaire, avec lesquels il est amené à coopérer, souhaitent disposer du plus grand nombre de renseignements possible.

Le présent décret, prenant en compte les missions dévolues par la loi à ces quatre autorités en matière de surveillance des dirigeants des établissements de crédit et des entreprises d'investissement, leur permettra d'avoir accès au bulletin n° 2 du casier judiciaire afin de compléter les informations dont elles pourraient déjà disposer dans la mesure où le bulletin n° 3 recense uniquement les condamnations à des peines privatives de liberté supérieures à deux ans et non assorties d'un sursis.

Le dispositif envisagé n'aboutit pas à enregistrer dans la base des informations issues du casier judiciaire national, mais uniquement la réponse électronique des services du casier.
Émet un avis favorable au projet de décret du Premier ministre modifiant l'article R. 79 du code de procédure pénale.

Délibération n° 01-050 du 10 juillet 2001 concernant la demande d'avis présentée par France Télécom relative à la présentation systématique aux services d'urgence du nom et de l'adresse correspondant au numéro de la ligne appelante

La Commission nationale informatique et libertés ;

Vu la Convention 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et notamment son article 5 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi susvisée ; Vu le nouveau code pénal ;

Vu la loi 96-659 du 26 juillet 1996 de réglementation des télécommunications, ensemble le décret n° 96-1225 du 27 décembre 1996 portant approbation du cahier des charges de France Télécom et le décret n° 96-1175 du 27 décembre 1996 relatif aux clauses types des cahiers des charges associés aux autorisations attribuées en application des articles L. 33-1 et L. 34-1 ;

Vu la loi n° 96-660 du 26 juillet 1996 relative à l'entreprise nationale France Télécom, ensemble le décret n° 96-1174 du 27 décembre 1996 approuvant les statuts de France Télécom et portant diverses dispositions relatives au fonctionnement de l'entreprise nationale ;

Vu les avis de la Commission concernant France Télécom n° 92-031 du 17 mars 1992 et n° 93-101 du 9 novembre 1993 relatifs respectivement à l'identification systématique des lignes appelant les pompiers par le 18 et le SAMU par le 15 et n° 96-011 du 12 mars 1996 relatif à la présentation du numéro de téléphone de la ligne appelante vers un appelé Numeris ou non Numeris, abonné au service ;

Saisie d'une demande d'avis relative à la mise en œuvre d'un traitement automatisé d'informations nominatives relatif à la présentation systématique aux services d'urgence (services départementaux d'incendie et de secours-SDIS, service d'aide médicale d'urgence-SAMU et police secours), du nom et de l'adresse correspondant au numéro de la ligne appelante ; **Formule les observations suivantes** :

Le traitement a pour objet de permettre aux services d'urgences (pompiers, SAMU, police secours) de bénéficier de la présentation systématique du nom et de l'adresse correspondant au numéro de la ligne par laquelle l'un de ces services est appelé, même si ce numéro figure en liste rouge ou sur une liste d'opposition rassemblant les personnes ne souhaitant pas paraître dans les services de recherche inversée ou d'annuaire inversé ou refusant la présentation de leur numéro de ligne à l'abonné qu'elles appellent.

Ce traitement répond à une demande formulée par les responsables des services concernés.

En mettant en place un tel traitement, France Télécom participe à l'exécution d'une mission de service public.

Il importe de rappeler que, sur avis favorables de la Commission nationale de l'informatique et des libertés, les services d'urgence précédemment cités sont déjà habilités à avoir connaissance, à l'occasion de tout appel dirigé vers eux, du numéro de la ligne appelante et que, par une procédure manuelle, ils sont fondés à obtenir auprès de France Télécom communication du nom et de l'adresse correspondant à ce numéro (cf. avis de la CNIL ci-dessus mentionnés).

La novation apportée par le traitement présenté consiste à faire l'économie de cette procédure manuelle et à la remplacer par un affichage instantané réalisé automatiquement par consultation et mise en oeuvre de l'annuaire inversé, au bénéfice des services d'urgence, du nom et de l'adresse correspondant à la ligne appelante.

La réalisation de cette opération sera assurée par un dispositif technique développé par les soins de la société France Télécom Intelmatique qui assurera également la connexion des services d'urgence aux bases de données annuaires de France Télécom.

Le recours à un annuaire inversé peut servir des intérêts légitimes, en particulier la sauvegarde de la vie humaine ainsi que des biens, par le moyen de la communication du nom et de l'adresse d'un abonné à des services d'urgence. Dans ces conditions, le traitement présenté apparaît légitime dans sa finalité et ses modalités de mise en œuvre.

Les seules informations traitées seront le numéro de téléphone de la ligne appelante, le nom et l'adresse correspondant à ce numéro de ligne ainsi que la date et l'heure de l'appel. Ces données ne seront conservées que le temps de leur transmission. Dans le cas d'abonnés figurant sur une liste d'opposition, ces données ainsi que l'identifiant du service d'urgence intéressé seront conservés pour des raisons de sécurité et de protection des personnes concernées durant une année.

Le traitement présenté visant à accroître l'efficacité de l'action des services d'urgence et compte tenu de leur mission de sauvegarde des personnes et des biens, aucune opposition ne pourra être formée contre la communication aux dits services d'urgences, du nom et de l'adresse du correspondant au numéro de la ligne appelant un numéro d'urgence SDIS (18), SAMU (15) et « police secours » (17).

Le dossier fait apparaître que toutes les mesures de sécurité nécessaires sont prévues dans l'exécution du traitement présenté.

La mise en œuvre de ce traitement s'accompagnera de mesures d'information, notamment dans les médias régionaux, dans un communiqué de presse France Télécom et dans la lettre d'information de France Télécom ainsi que dans les pages d'information générale des annuaires édités par cette société ; par ailleurs, lors de la souscription de tout nouveau contrat d'abonnement ou de toute adhésion au dispositif des listes d'opposition, une information sera délivrée précisant que l'opposition concernée ne pourra pas s'appliquer aux services d'urgence sus-visés.

Émet un avis favorable à la mise en œuvre du traitement objet de la présente demande d'avis.

Délibération n° 01-051 du 9 octobre 2001 relative aux échanges d'informations mis en place entre la direction générale des impôts et les chambres de métiers

(Demande d'avis n° *714861,* demande d'avis modifïcative n° 104960)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis :

— par le ministère de l'Économie, des Finances et de l'Industrie d'un projet d'arrêté « modifiant l'arrêté du 22 septembre 1989 autorisant la création d'un traitement automatisé de calcul de taxe professionnelle » par la direc tion générale des impôts (DGI) ;

— par l'assemblée permanente des chambres de métiers d'un projet « d'acte réglementaire-cadre relatif au rapprochement entre les répertoires des métiers et les fichiers des assujettis à la taxe pour frais de chambres de métiers », portant création d'un modèle type auquel pourront se référer les chambres de métiers ;

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

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu le Livre des procédures fiscales, notamment les articles L. 113, L. 135 B, L. 135 J et R.* 135 B-1 à R.* 135 B-4;

Vu le titre il du code de l'artisanat ;

Vu le décret n° 66-137 du 7 mars 1966 modifié, relatif à l'assemblée permanente des chambres de métiers ;

Vu le décret n° 98-247 du 2 avril 1998 relatif à la qualification artisanale et au répertoire des métiers ;

Vu l'arrêté du 22 septembre 1989 autorisant la création d'un traitement informatisé de calcul de taxe professionnelle, modifié par arrêtés des 8 mars 1996 et 14 novembre 1996 ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle en son rapport et Monsieur Michel Capcarrère, commissaire du Gouvernement adjoint, en ses observations ; **Rend l'avis suivant :**

Sur la finalité et le fondement juridique des traitements

Les projets d'actes réglementaires sur lesquels la Commission est appelée à se prononcer visent à autoriser la mise en place d'échanges d'informations entre les services fiscaux et les chambres de métiers, afin de permettre aux organismes consulaires d'apporter une aide au recensement des assujettis à la taxe pour frais de chambres de métiers (TCM), due par les entreprises indi-

viduelles et les sociétés qui sont immatriculées, à titre obligatoire ou sur leur demande, au répertoire des métiers.

Le dispositif envisagé a pour objet d'autoriser le rapprochement, par les chambres de métiers et à leur initiative, de la liste des assujettis à la TCM transmise par la DGI avec le répertoire des métiers dont elles assurent la tenue, afin d'identifier les différences existant entre les deux fichiers, de les signaler aux services fiscaux compétents, et ainsi de faire disparaître les divergences injustifiées.

Les flux d'informations envisagés trouvent leur fondement juridique dans l'article L. 135 J du Livre des procédures fiscales (LPF) qui prévoit, par dérogation à la règle du secret professionnel en matière fiscale, que :

« Afin de procéder à des rapprochements avec le répertoire des métiers, les chambres de métiers peuvent se faire communiquer par l'administration fiscale la liste nominative des assujettis à la taxe pour frais de chambres de métiers.

« Les chambres de métiers et l'administration peuvent se communiquer mutuellement les informations nécessaires au recensement des assujettis à la taxe pour frais de chambres de métiers.

« Les dispositions du cinquième alinéa de l'article L. 135 B sont applicables aux informations ainsi transmises.

« La *Commission estime que les projets d'actes réglementaires qui lui sont soumis doivent déterminer plus précisément les finalités du traitement des informations. En outre, l'acte réglementaire de l'APCM devrait rappeler l'interdiction d'utilisation à d'autres fins, notamment commerciales, politiques ou électorales, des informations reçues de l'administration fiscale.*

« À ce titre, la finalité du traitement devrait être définie comme suit dans l'acte réglementaire de l'APCM : "Le traitement a pour finalité d'identifier les différences entre le répertoire des métiers et le fichier des assujettis à la taxe pour frais de chambres de métiers et ainsi, d'aider à la suppression des différences injustifiées de la liste des assujettis. Les informations provenant de l'administration fiscale ne peuvent faire l'objet d'aucune autre utilisation".

« En outre, l'alinéa e du 4 de l'article 1e du projet d'arrêté ministériel, qui modifie l'article 5 de l'arrêté du 22 septembre 1989 susvisé, devrait être remplacé par un 4 bis, ainsi rédigé : "La liste des assujettis à la taxe pour frais de chambres de métiers est communiquée, au titre de l'année en cours, aux chambres de métiers qui le demandent, afin de leur permettre de procéder à des rapprochements avec le répertoire des métiers, d'identifier les différences entre ces fichiers et ainsi, d'aider à la suppression des différences injustifiées de la liste des assujettis". »

Sur les informations échangées

Chaque chambre de métiers — à l'exclusion des chambres régionales qui n'interviennent pas dans la tenue du répertoire des métiers — pourra demander à la direction des services fiscaux de sa circonscription à avoir communication, sur papier ou support informatique, de la liste des personnes et sociétés qui sont redevables de la TCM.

La *Commission précise que les fichiers transmis par l'administration fiscale devront tenir compte des limites des circonscriptions des chambres des métiers, notamment pour celles dont le champ de compétence ne correspond*

pas à un département, afin que chaque organisme ne dispose que des informations concernant les artisans situés dans son ressort territorial.

Les informations susceptibles d'être communiquées aux organismes consulaires sont le n° SIRET, l'identité de l'exploitant ou la raison sociale de la société ainsi que les adresses des lieux d'imposition, notamment celles des établissements secondaires, à l'exclusion de toute autre donnée telle que la nature des droits acquittés — droit fixe ou additionnel de la TCM — ou le montant de la taxe.

En réponse, les chambres de métiers pourront faire parvenir à l'administration fiscale deux catégories de discordances qu'elles auront détectées entre le fichier des assujettis à la TCM et le répertoire des métiers :
— la liste des anomalies ou différences constatées entre les deux fichiers qui concernent les données d'identification et d'adresse des entreprises artisa nales ;
— la liste des entreprises immatriculées au répertoire des métiers qui ne sont pas recensées par l'administration fiscale en tant que redevable de la TCM.

Ces informations seront exploitées dans les centres des impôts et pourront donner lieu à l'émission de rôles supplémentaires.

La *Commission constate que les informations échangées sont adéquates, pertinentes et non excessives pour permettre aux organismes consulaires d'apporter aux services fiscaux une aide au recensement des assujettis à la TCM.*

Sur la durée de conservation des informations

L'article 5 du projet d'acte réglementaire de l'APCM prévoit que les chambres de métiers pourront conserver les informations reçues « au plus pendant un an [...], le temps de réaliser le traitement et de fournir les résultats aux centres des impôts ».

La Commission demande que la rédaction de cet article soit précisée comme suit : « les informations transmises par l'administration fiscale ou résultant de leur traitement ne font l'objet d'aucune conservation par les chambres de métiers à l'issue de la transmission aux centres des impôts de la liste prévue à l'article 4. »

Sur les mesures de sécurité à adopter par les chambres de métiers

En vertu de l'article L. 135 B du LPF susmentionné, les informations échangées entre les chambres de métiers et l'administration fiscale sont couvertes par le secret professionnel et soumises aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Leur utilisation doit, en outre, respecter les obligations de confidentialité et de sécurité, précisées par les articles R.* 135 B-1 à R.* 135 B-4 du LPF, dont il résulte, en ce qui concerne les chambres de métiers, que :
— l'autorité destinataire des informations fiscales est le président de la chambre de métiers ou la personne déléguée à cet effet par le président ;
— elle désigne, s'il y a lieu, le personnel administratif habilité à utiliser ces informations ;
— les chambres de métiers ne peuvent ni communiquer, ni céder à un tiers les informations traitées sous forme nominative ;

— l'autorité destinataire prend toutes mesures utiles pour assurer la sécurité des documents et informations transmis par l'administration fiscale et en em pêcher une utilisation détournée ;
— elle informe les personnes qui utilisent les informations ou en ont connais sance, des peines encourues en cas de rupture du secret professionnel, qui sont fixées par l'article 226-13 du code pénal.

La Commission demande que l'acte réglementaire de l'APCM comporte le visa des articles R.* 135 B-1 à R.* 135 B-4 du Livre des procédures fiscales et qu'un nouvel article soit ajouté, ainsi rédigé : « l'autorité destinataire des informations fiscales est le président de la chambre de métiers ou la personne déléguée à cet effet par le président. Cette autorité prend toutes mesures utiles pour assurer la sécurité des documents et informations transmis par l'administration et en empêcher une utilisation détournée. »

La Commission demande également qu'une instruction de l'APCM informe les chambres de métiers des précautions dont doivent être entourés les trans ferts d'informations avec l'administration fiscale.

Sur l'information des personnes concernées

En ce qui concerne les modalités d'information des personnes sur lesquelles portent les échanges de données, la Commission demande :
— que les avis d'imposition à la taxe professionnelle — qui mentionnent également les taxes qui lui sont annexées, parmi lesquelles la TCM — infor ment, à l'avenir, les contribuables de la transmission aux chambres de mé tiers, sur leur demande, de la liste des assujettis à la taxe pour frais de chambres de métiers ;
— que les artisans se faisant immatriculer au répertoire des métiers ou de mandant la modification des informations les concernant qui y figurent soient systématiquement informés par les chambres de métiers de la possibi lité de transmission à l'administration fiscale des informations inscrites au ré pertoire.

Sur la procédure à suivre devant la CNIL

Il est prévu que les chambres de métiers souhaitant coopérer avec l'adminis tration fiscale dans les conditions fixées par le modèle type de l'APCM, adresseront à la Commission une déclaration simplifiée de conformité audit modèle type.

Au bénéfice de ces observations, la Commission émet un avis favorable sur le projet d'arrêté modificatif du ministre de l'Économie, des Finances et de l'Industrie relatif au traitement « Taxe Professionnelle », **sous réserve** :
— qu'à l'article 1er, l'alinéa e du 4 de l'article 5 de l'arrêté du 22 sep tembre 1989 soit remplacé par un 4 bis, ainsi rédigé : « La liste des assujet tis à la taxe pour frais de chambres de métiers est communiquée, au titre de l'année en cours, aux chambres de métiers qui le demandent, afin de leur permettre de procéder à des rapprochements avec le répertoire des métiers, d'identifier les différences entre ces fichiers et ainsi, d'aider à la suppression des différences injustifiées de la liste des assujettis. » ;
— que la mention suivante soit portée sur les avis d'imposition à la taxe pro fessionnelle : « la liste des assujettis à la taxe pour frais de chambres de mé-

tiers est communiquée, sur leur demande, aux chambres de métiers, afin d'en assurer la concordance avec le répertoire des métiers. » ;

et **un avis favorable sur le projet d'acte réglementaire de l'assemblée permanente des chambres de métiers, sous réserve** :
— que texte comporte le visa des articles R.* 135B-1 à R.* 135 B-4 du Livre des procédures fiscales ;
— que la finalité du traitement de l'APCM soit définie comme suit : « le trai tement a pour finalité d'identifier les différences entre le répertoire des mé tiers et le fichier des assujettis à la taxe pour frais de chambres de métiers et ainsi, d'aider à la suppression des différences injustifiées de la liste des assu jettis. Les informations reçues de l'administration fiscale ne peuvent faire l'objet d'aucune autre utilisation » ;
— qu'un nouvel article précise : « l'autorité destinataire des informations fis cales est le président de la chambre de métiers ou la personne déléguée à cet effet par le président. Cette autorité prend toutes mesures utiles pour as surer la sécurité des documents et informations transmis par l'administration et en empêcher une utilisation défournée » ;
— que l'article 5 soit ainsi modifié : « les informations transmises par l'ad ministration fiscale ou résultant de leur traitement ne font l'objet d'aucune conservation par les chambres de métiers à l'issue de la transmission aux centres des impôts de la liste prévue à l'article 4 » ;
— que l'APCM informe les chambres de métiers par voie de circulaire sur les précautions dont doivent être entourés les transferts d'informations avec l'administration fiscale ;
— que les artisans qui se font immatriculer au répertoire des métiers soient systématiquement informés par les chambres de métiers sur la possibilité que des informations les concernant soient transmises à l'administration fiscale aux fins d'aide au recensement des assujettis à la taxe pour frais de cham bres de métiers.

Délibération n° 01-052 du 18 octobre 2001 portant avis sur deux projets d'arrêtés présentés par le ministère de la Justice modifiant les arrêtés des 18 juin 1986 et 13 avril 1993 relatifs à la mise en œuvre, dans les tribunaux de grande instance, d'un système de gestion automatisée des procédures

(Demande d'avis n° 103727)

La Commission nationale de l'informatique et des libertés ;

Vu la Convention 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 le code pénal et le code de procédure pénale ;

Vu la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978;

Vu le décret n° 90-115 du 2 février 1990 portant application aux juridictions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 précitée ;

Vu les arrêtés du garde des Sceaux des 18 juin 1986 et 13 avril 1993 ;

Vu la délibération de la CNIL n° 86-57 du 20 mai 1986 ;

Vu les projets d'arrêté présentés par le garde des Sceaux, ministre de la Justice ;

Après avoir entendu Monsieur Gérard Gouzes, vice-président, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Saisie par le ministre de la Justice de deux projets d'arrêté modifiant les arrêtés des 18 juin 1986 et 13 avril 1993 relatifs à la mise en oeuvre, dans les tribunaux de grande instance, d'un modèle-type de traitement automatisé des procédures pénales relevant des procureurs de la République et des juges d'instruction, des procédures pénales et civiles des juges des enfants ainsi que des affaires civiles, administratives et commerciales relevant des procureurs de la République ;

Formule les observations suivantes :

Les projets d'arrêtés modificatifs dont est saisie la Commission ont pour objet de compléter les arrêtés des 18 juin 1986 et 13 avril 1993 relatifs à la mise en oeuvre, dans les tribunaux de grande instance, d'un système de gestion automatisée des procédures, par un article 6 fixant les modalités de conservation et de mise à jour des informations traitées.

La présentation de ces projets d'arrêtés fait suite à un arrêt rendu par le Conseil d'État le 27 juillet 2001 aux termes duquel la haute juridiction a jugé que les arrêtés des 18 juin 1986 et 13 avril 1993 sont entachés d'illégalité pour n'avoir pas pris en compte « les mesures propres à assurer le respect des conditions ou réserves » figurant dans l'avis préalable de la Commission du 20 mai 1986.

La CNIL avait en effet rappelé, d'une part, que les informations relatives à la gestion des procédures pénales ne devraient pas être conservées sur support informatique plus de cinq années à compter du jugement définitif ou de la décision de classement et que les informations devront faire l'objet d'une mise à jour à la suite des mesures d'amnistie, de réhabilitation ou de grâce et, d'autre part, que les informations relatives à la gestion des affaires relevant des attributions non répressives du parquet ne devraient pas être conservées au-delà du temps nécessaire à l'exercice des contrôles pour lesquelles elles ont été enregistrées.

Le nouvel article inséré dans chaque arrêté prévoit en premier lieu que les informations relatives aux procédures pénales « sont conservées pendant une durée égale aux délais légaux de prescription de la peine mais n'excédant pas cinq ans à compter au jugement définitif ou de la décision de classement ».

S'agissant en second lieu des informations relatives à la gestion des affaires relevant des attributions non répressives du parquet, les deux projets d'arrêtés, reprenant la rédaction de la délibération de la Commission du 20 mai 1986, précisent qu'elles « ne sont pas conservées sur support informatique au-delà du temps nécessaire à l'exercice des contrôles pour lesquels elles ont été enregistrées ». Les deux projets d'arrêtés ajoutent que, pour ces catégo-

ries d'informations, la durée de conservation sur support informatique n'excédera pas, en tout état de cause, cinq ans.

Émet un avis favorable aux projets d'arrêtés modifiant les arrêtés des 18 juin 1986 et 13 avril 1993 soumis par le garde des Sceaux, ministre de la Justice.

Délibération n° 01-053 du 18 octobre 2001 portant avis sur une expérimentation du Conseil national d'information géographique relative à la faisabilité d'un fichier national de référence de « points géographiques à l'adresse »

(Demande d'avis n° *759755)*

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le président du CNIG d'une expérimentation sur la commune de Colomiers relative à la faisabilité d'un fichier national de référence de « points géographiques à l'adresse » ;

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

Vu la directive n° 95/46/CE du parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

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

Vu la loi n°51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 ;

Vu le décret n° 85-790 du 26 juillet 1985 modifié portant statut du CNIG ;

Vu le projet de décision du président du CNIG portant création du traitement ;

après avoir entendu monsieur Didier Gasse, commissaire en son rapport et madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :

Sur la finalité du traitement

La Commission est saisie par le Conseil national de l'information géographique (CNIG), instance consultative placée auprès du ministre chargé de l'Équipement, d'une demande d'avis relative à la création d'un traitement automatisé sur la commune de Colomiers associant à chaque adresse une coordonnée géographique.

Ce traitement est destiné à apprécier la faisabilité d'un fichier de référence national de points géographiques à l'adresse.

Sur *la constitution du traitement*

Ce traitement serait constitué à partir de la comparaison de fichiers d'adresses sur la commune de Colomiers qui seraient mis à la disposition du CNIG par la direction générale des impôts, l'INSEE, EDF-GDF, France Télécom et la commune de Colomiers, après avoir été anonymisés par chacun des responsables de ces traitements.

L'exploitation des informations ainsi communiquées serait effectuée par La Poste et l'Institut géographique national.

Sur la nature des informations traitées

Les informations contenues dans le fichier issu de la comparaison des fichiers fournis par les organismes précités sont ceux définis aux lignes 3,4,5 et 6 de l'adresse aux termes de la norme AFNOR XP Z 10-011 (mai 1997) c'est-à-dire :

— ligne 3 : bâtiment, accès au bâtiment, ensemble immobilier ;
— ligne 4 : n° dans la voie, type de voie, nom de la voie ;
— ligne 5 : lieu-dit ;
— ligne 6 : code postal et ville.

En outre, chaque adresse physique se verra attribuer ses références géographiques exactes à partir de la base de données Géoroute de l'IGN.

Sur la durée de conservation du fichier

Ce fichier sera conservé jusqu'au printemps 2002, date de la présentation des résultats de l'application en séance plénière du CNIG.

Le droit d'accès et de rectification prévu par les articles 34 et 36 de la loi n° 78-17 du 6 janvier 1978 s'exerce auprès du CNIG.

Compte tenu de ces observations :

Émet un avis favorable au projet de décision, sous réserve qu'il prenne la forme d'un arrêté du ministre chargé de l'Equipement publié au Journal officiel, étant admis que la Commission sera associée au déroulement de l'expérimentation et destinataire de ses résultats.

Délibération n° 01-056 du 13 novembre 2001 relative au projet d'arrêté présenté par la mairie de Paris portant création d'un traitement ayant pour finalité le suivi des candidatures et la gestion administrative du Conseil de la citoyenneté des parisiens non communautaires

(Demande d'avis n° 773820)

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

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 pris pour son application ;

Vu la loi n° 92-125 du 6 février 1992 relative à l'administration territoriale de la République ;

Vu le code général des collectivités territoriales, notamment ses articles L. 2121-1 et L. 2143-2;

Vu le projet de délibération du Conseil du Paris portant création du Conseil de la citoyenneté des parisiens non communautaires ;

Vu le projet d'arrêté présenté par la mairie de Paris portant création d'un traitement ayant pour finalité le suivi des candidatures et la gestion administrative du Conseil de la citoyenneté des parisiens non communautaires ;-

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Saisie par la mairie de Paris d'un projet d'arrêté relatif à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité de faciliter l'enregistrement et le suivi des candidatures ainsi que la mise en place et la gestion administrative du « Conseil de la citoyenneté des parisiens non communautaires » ;

Formule les observations suivantes :

La mairie de Paris souhaite instituer un conseil consultatif des résidents étrangers à Paris, hors ressortissants de l'Union européenne, intitulé « Conseil de la citoyenneté des parisiens non communautaires ». La création de ce conseil se fonde sur les dispositions de l'article L. 2143-2 du code général des collectivités territoriales (CGCT)) qui précise qu'un « conseil municipal peut créer des comités consultatifs sur tout problème d'intérêt communal concernant tout ou partie du territoire de la commune. Ces comités comprennent des personnes qui peuvent ne pas appartenir au conseil, notamment des représentants des associations locales ».

Cet article dispose également que « Les comités peuvent être consultés par le maire sur toute question ou projet intéressant les services publics et équipements de proximité et entrant dans le domaine d'activité des associations membres du comité. Ils peuvent par ailleurs transmettre au maire toute proposition concernant tout problème d'intérêt communal pour lequel ils ont été institués ».

Le Conseil de la citoyenneté des parisiens non communautaires aura pour mission de :

— donner des avis sur toute question intéressant la vie à Paris des résidents étrangers non ressortissants d'un pays de l'Union européenne et entrant dans le champ de compétence du Conseil de Paris ;

— formuler et transmettre au maire des propositions sur toutes les questions municipales concernant les Parisiens non ressortissants d'un pays de l'Union européenne.

Ce conseil sera composé de ressortissants étrangers (quatre-vingt-dix titulaires et trente suppléants) désignés par le maire de Paris à partir d'une liste constituée de personnes s'étant portées candidates et remplissant les conditions suivantes : être non ressortissants de pays de l'Union européenne, ne pas disposer de la double nationalité française et étrangère, être en situa-

tion régulière, être âgé d'au moins 18 ans, et être installé à Paris depuis un an, soit avant le 31 décembre 2000.

Les personnes intéressées sont invitées à faire acte de candidature en adressant, à l'adjointe au maire de Paris chargée de l'intégration, un formulaire précisant leur nationalité, leur identité, leur date et lieu de résidence à Paris, leur sexe, leur appartenance à une association, leur participation à des actions au service de la collectivités et leur (s) motivation (s).
Ces candidatures seront examinées par une commission composée d'élus parisiens et de personnalités qualifiées, les maires d'arrondissements étant consultés pour les candidats qui résident dans leur arrondissement.

Le traitement informatique faisant l'objet du présent avis est destiné à faciliter l'examen des dossiers par la commission de candidature, à permettre l'édition de listes destinées aux maires d'arrondissement, l'envoi de courriers aux candidats non retenus et à assurer la gestion des convocations des membres titulaires ou suppléants aux séances du conseil.

La Commission estime que la finalité du traitement, circonscrite à ces seules opérations, est légitime.

La mairie de Paris prévoit l'enregistrement dans le traitement des nom, prénoms, sexe et date de naissance, de l'adresse et de la date de résidence à Paris, de la nationalité, de l'activité professionnelle, de l'appartenance à une association, des actions au service de la collectivité ainsi que du degré de motivation.
La Commission prend acte du fait que l'information sur la nationalité sera uniquement utilisée pour déterminer la zone géographique du pays dont le candidat est ressortissant, selon la nomenclature INSEE, et permettre la répartition des sièges au sein du conseil en fonction de l'importance relative, dans chaque arrondissement, des ressortissants étrangers. La Commission prend également acte que la régularité du séjour est une condition requise pour être membre du conseil ; qu'en tout état de cause, aucune information sur ce point ne sera enregistrée dans le traitement.
Le recueil des informations relatives aux éventuelles actions du candidat au service de la collectivité ainsi que son éventuelle appartenance à une association, est également pertinent au regard de la finalité du traitement.

En revanche, la détermination, par les services de la mairie, du degré de motivation établi à partir des éléments fournis par les candidats sur les formulaires de déclarations, ne paraît pas pertinente. Aussi, la Commission estime-t-elle que l'information relative au degré de motivation prêté au candidat ne doit pas figurer dans le traitement.
Enfin, dans la mesure où certaines informations recueillies sur les formulaires de candidatures sont susceptibles de relever directement ou indirectement de l'article 31 de la loi du 6 janvier 1978, il y a lieu de souligner que la conservation en mémoire informatique des informations considérées, fût-ce pour le temps limité du traitement des candidatures, est subordonnée au recueil de l'accord exprès des intéressés.
La Commission prend acte de ce que les données relatives aux candidatures ne seront conservées que jusqu'à la date de l'institution du Conseil de la citoyenneté des parisiens non communautaires, les données concernant les candidatures non retenues devant être supprimées du fichier aussitôt le conseil mis en place. Les données concernant les membres désignés seront

conservées pendant la durée de la mandature, soit un an renouvelable chaque année.

Les destinataires de ces informations seront :
— le maire de Paris ;
— l'adjointe au maire, chargée de l'intégration et des étrangers non com munautaires, ainsi que ses services qui recevront les déclarations de candi datures et assureront leur enregistrement sur des micro-ordinateurs accessibles aux seuls agents du service ;
— les membres de la commission de candidature désignés par le maire de Paris qui auront accès aux données issues du traitement et aux fiches de can didatures ;
— les maires d'arrondissement, pour les candidats résidant dans l'arrondis sement concerné, et ce sous forme de liste nominative pour leur permettre de formuler leurs avis sur les candidatures.

La Commission prend acte que les candidats seront informés, conformément à l'article 27 de la loi du 6 janvier 1978, de l'informatisation de leur déclaration, des destinataires des informations et des conditions d'exercice de leur droit d'accès et de rectification.
Dès lors, et au regard des dispositions de la loi du 6 janvier 1978, le traitement automatisé d'informations nominatives tel que présenté à la Commission nationale de l'informatique et des libertés n'appelle pas d'observations particulières.
La Commission émet un avis favorable au projet d'arrêté présenté par la ville de Paris relatif à la création d'un traitement ayant pour finalité l'enregistrement et le suivi des candidatures ainsi que la mise en place et la gestion administrative du « Conseil de la citoyenneté des parisiens non-communautaires » **sous réserve** :
— de l'adoption de la délibération par le Conseil de Paris instituant le dit conseil ;
— de la suppression de la rubrique informatique sur les degrés de motiva tion prêtés aux candidats.

Délibération n° 01-058 du 11 décembre 2001 portant avis favorable sur le projet d'arrêté présenté par l'INSEE, portant sur la diffusion des résultats du RGP 1999, et modifiant l'arrêté du 22 mai 1998

(Demande d'avis n° 555642)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le directeur général de l'INSEE d'un projet d'arrêté portant modification de l'arrêté du 22 mai 1998 relatif à la création d'un traitement automatisé réalisé à l'occasion de la collecte et de la diffusion des résultats du recensement général de la population ;

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

Vu la directive n° 95/46/CE du parlement européen et du conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du

traitement des données à caractère personnel et à la libre circulation des données ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier susvisée ;

Vu l'arrêté du 22 mai 1998 portant création d'un traitement automatisé réalisé à l'occasion de la collecte et de la diffusion des résultats du recensement général de la population de 1999 ;
Vu le projet d'arrêté du directeur général de l'INSEE portant modification de l'arrêté susvisé de 1998 ;
Après avoir entendu Guy Rosier, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :
La Commission est saisie par l'INSEE d'un projet d'arrêté portant modification des modalités de diffusion des résultats du recensement général de la population de 1999.

Le projet a pour objet de modifier les articles 8, 9 et 10 de l'arrêté du 22 mai 1998 :
— En premier lieu, l'INSEE sollicite l'autorisation de diffuser des fichiers de données individuelles anonymisées à un seuil d'au moins 50 000 habitants mais sur des zones qui ne seraient pas d'un seul tenant.

La modification se traduit par la suppression, à l'alinéa 11 de l'article 8 et à l'alinéa I de l'article 9 des mots « d'un seul tenant ».

Il apparaît, compte tenu du niveau d'agrégation considéré en l'espèce — soit 50 000 — que cette modification ne soulève pas de difficulté particulière, sous la réserve qu'il ne soit plus dès lors fait référence à une zone géographique mais à un seuil de 50 000 habitants.

De surcroît l'INSEE a décidé la mise en oeuvre d'un registre national des cessions de fichiers de données individuelles anonymisées relatifs à une zone géographique d'au moins 50 000 habitants (ajoût d'un alinéa IV à l'article 9).

Ce registre qui mentionnerait les zonages concernés, les demandeurs ainsi que les licences d'usage délivrées, a pour objectif de renforcer la protection de la confidentialité des données en évitant qu'un même organisme puisse obtenir plusieurs fichiers géographiquement comparables et l'empêcher ainsi d'effectuer des recoupements entre des fichiers obtenus successivement.
La tenue de ce répertoire est de nature à apporter des garanties en ce qui concerne les cessions réalisées, qu'elles portent sur des zones d'un seul tenant ou non.
— L'INSEE sollicite en deuxième lieu la possibilité de diffuser d'une part des tableaux ne comportant pas de variables sensibles sur des zonages adminis tratifs d'un seul tenant d'au moins 6 000 habitants (alinéa II de l'article 10), d'autre part, de diffuser des tableaux répartissant la population par nationa lité et par pays de naissance pour les arrondissements, zones d'emploi, aires urbaines, unités urbaines et zones définies pour la politique de la ville ou

leurs regroupements à partir d'un seuil de 10 000 habitants, ces niveaux de seuil pouvant ne pas correspondre aux quartiers prédéfinis dits « IRIS » (alinéa III de l'article 10).

Ces diffusions ont pour but de répondre à des besoins de connaissance générale de la population sur toutes ces zones. Dans la mesure où ces diffusions se présenteront sous forme de tableaux et ou les niveaux de seuil seront fixés respectivement à 6000 et 10 000 habitants, la demande présentée par l'INSEE n'appelle pas d'objection de la Commission.

— L'INSEE sollicite en troisième lieu la diffusion de fichiers individuels non nominatifs résultant d'un sondage au 1/20^{e}, dits « fichiers d'études », soit au niveau de la commune, soit au niveau du quartier fixe « IRIS 2000 » (ajout d'un alinéa III à l'article 9).

Ces fichiers ne concerneraient qu'un ménage sur vingt. Les cessions réalisées feraient l'objet d'un engagement du bénéficiaire de les utiliser à des fins exclusives d'étude ou de recherche, et excluraient toute identification directe ou indirecte des personnes. Elles seraient portées dans le registre des cessions.

Compte tenu de l'ensemble des précautions prises par l'INSEE lors de la cession de ces fichiers, la demande est recevable.

Toutefois, il convient de modifier la rédaction de l'alinéa III de l'article 9 pour remplacer la notion d'individus par celle de ménages

Compte tenu de ces observations, émet un avis favorable au projet d'arrêté portant modification de l'arrêté du 22 mai 1998, sous réserve que :

— l'alinéa III de l'article 9 soit rédigé comme suit : « des fichiers de données individuelles anonymes, lorsqu'ils résultent d'un sondage portant sur 1/20^{e} des ménages, au maximum, peuvent être cédés » ;

— à l'alinéa II de l'article 9 les mots « s'ils sont relatifs à une zone géographique d'au moins 50 000 habitants » soient remplacés par les mots « s'ils concernent au moins 50 000 habitants ».

Délibération n° 01-062 du 20 décembre 2001 modifiant la norme simplifiée n° 20 concernant les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social

La Commission nationale de l'informatique et des libertés ;

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 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

Vu le décret n° 78-774 du 17 juillet 1978 modifié, pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu la délibération n° 97-005 du 21 janvier 1997 concernant les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social ;

Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Après avoir effectué diverses missions de vérification sur place auprès de bailleurs sociaux, la Commission, afin de s'assurer des conditions de mise en oeuvre des traitements automatisés d'informations nominatives, souhaite apporter deux modifications à la norme simplifiée n° 20.

La première modification consiste à préciser que l'information relative à la nationalité des demandeurs de logement, dont la collecte est autorisée depuis 1984 à l'occasion des procédures d'attribution de logements, n'a pas à faire l'objet d'interrogations répétées auprès des locataires une fois dans les lieux.

Tout particulièrement, les textes législatifs et réglementaires régissant les enquêtes d'occupation des logements sociaux et les enquêtes relatives au supplément de loyer solidarité ne prévoient pas la collecte de cette information auprès des locataires. .

Par ailleurs, la nécessaire mise à jour des fichiers ne saurait justifier que les locataires soient fréquemment interrogés sur ce point, fût-ce de manière facultative, les intéressés concernés qui viendraient à changer de nationalité pouvant, à tout moment, demander que cette information soit rectifiée, conformément aux dispositions de l'article 36 de la loi.

La deuxième modification vise à fixer la durée de conservation des informations relatives aux demandeurs de logement qui, aux termes de la norme simplifiée adoptée en 1997, ne peut excéder une année à compter de la date de dépôt ou de renouvellement de la demande. En pratique cependant, les demandeurs de logement pouvant maintenir leur demande durant de nombreuses années après la demande d'origine, il y a lieu d'éviter que la norme simplifiée ait pour effet d'alourdir excessivement, au regard de l'intérêt des demandeurs de logement, les procédures à mettre en oeuvre ; En conséquence :

L'article 3 a) de la norme est complété par la phrase suivante :

L'information relative à la nationalité ne peut pas être collectée à l'occasion des enquêtes relatives au supplément de loyer solidarité ou des enquêtes d'occupation des logements sociaux effectuées dans le cadre de la présente norme.

L'article 4 de la norme est rédigé ainsi :

Les informations relatives aux locataires en place ne doivent pas être conservées après le règlement du solde de l'intéressé à l'exception des informations nécessaires à l'accomplissement des obligations légales.
Les informations relatives aux demandeurs de logement ne doivent pas être conservées au-delà de cinq années à compter de la date de dépôt ou de renouvellement de la demande. Elles doivent être effacées si, au cours de ce délai, les personnes intéressées en font la demande et, en tout état de cause, dès qu'elles ont obtenu l'attribution d'un logement.

Annexe 6

Décisions des juridictions

ARRÈT DU CONSEIL D'ÉTAT DU 30 MAI 2001
(Req. n° 218108)

Le Conseil d'État statuant au contentieux

Vu la requête, enregistrée le 1e mars 2000 au secrétariat du contentieux du Conseil d'État, présentée par M. X, demeurant... en Suisse ; M. X demande au Conseil d'État :
1) d'annuler pour excès de pouvoir la décision implicite par laquelle la Commission nationale de l'informatique et des libertés a refusé de lui communiquer les informations le concernant figurant dans le fichier système d'information Schengen, de faire rectifier ces informations et de notifier aux tiers ces modifications ;
2) d'enjoindre à la Commission nationale de l'informatique et des libertés de lui communiquer les informations le concernant contenues dans le système d'information Schengen, de faire rectifier ces informations et de notifier ces rectifications aux tiers ;
3) de condamner la Commission nationale de l'informatique et des libertés à lui rembourser les frais qu'il a exposés ;

Vu les autres pièces du dossier ;

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

Vu le décret n° 95-304 du 21 mars 1995 portant publication de la convention d'application de l'accord de Schengen du 14 juin 1985 signée à Schengen le 19 juin 1990 ;

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 Herondart, auditeur ;
— les conclusions de Mme Maugüé, commissaire du gouvernement ;

Considérant, d'une part, qu'aux termes des stipulations du premier paragraphe de l'article 109 de la convention d'application de l'accord de Schengen signée le 19 juin 1990 : « le droit de toute personne d'accéder aux données la concernant qui sont intégrées dans le système d'information Schengen s'exerce dans le respect du droit de la partie contractante auprès de laquelle elle le fait valoir. Si le droit national le prévoit, l'autorité nationale de contrôle prévue à l'article 114 paragraphe 1 décide si des informations sont communiquées et selon quelles modalités [...] » ; que, selon les stipulations du premier paragraphe de l'article 114 de la même convention : « 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'aux termes du second paragraphe du même article : « 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 [...] » ;

Considérant, d'autre part, que l'article 34 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que toute personne justifiant de son identité a le droit d'interroger les services ou organismes qui détiennent des fichiers si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication ; que les articles 35 et 36 de la même loi accordent au titulaire du droit d'accès organisé par l'article 34 un droit de communication de ces informations, ainsi que le droit d'en obtenir le cas échéant, la rectification ou l'effacement ; qu'aux termes de l'article 38 : « si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par la Commission » ; que, selon l'article 39 : « en ce qui concerne les traitements intéressant la sûreté de l'État, la défense et la sécurité publique, la demande est adressée à la Commission qui désigne l'un de ses membres [...] pour mener toutes investigations utiles et faire procéder aux modifications nécessaires [...]. Il est notifié au requérant qu'il a été procédé aux vérifications » ;

Sur les conclusions dirigées contre la décision implicite de la Commission nationale de l'informatique et des libertés en tant qu'elle refuse de faire procéder aux modifications des informations concernant le requérant dans le système d'information Schengen :

Considérant que, postérieurement à l'introduction de la présente requête, la Commission nationale de l'informatique et des libertés a désigné, conformément à l'article 39 de la loi du 6 janvier 1978, un de ses membres pour procéder aux vérifications des informations concernant M. X contenues dans le système d'information Schengen ; que la Commission nationale de l'informatique et des libertés a procédé à ces vérifications et, après autorisation du ministre de l'Intérieur, a informé le requérant, par lettre du 15 mai 2000, qu'il avait été procédé au retrait de son signalement dans le système d'information Schengen ; qu'il ressort des pièces du dossier que, contrairement à ce que soutient M. X, ce retrait a effectivement eu lieu ; que, dès lors, les conclusions dirigées contre la décision implicite de la Commission nationale de l'informatique et des libertés en tant qu'elle aurait refusé de faire procéder aux modifications des informations concernant le requérant dans le système d'information Schengen et tendant à ce qu'il soit enjoint à la Commission de faire procéder à ces modifications sont devenues sans objet ; qu'il n'y a, dès lors, pas lieu d'y statuer ;

Sur les conclusions dirigées contre la décision implicite de la Commission nationale de l'informatique et des libertés en tant qu'elle refuse de communiquer au requérant les informations le concernant contenues dans le fichier système d'information Schengen et de notifier les modifications aux tiers :

Considérant qu'il résulte des stipulations des articles 109 et 114 de la convention d'application de l'accord de Schengen que le droit d'accès au fichier système d'information Schengen s'effectue dans le cadre du droit national du pays dans lequel s'effectue la demande ; que l'article 39 de la loi du 6 janvier 1978 limite l'accès aux traitements intéressant la sûreté de l'État, la défense et la sécurité publique à un droit d'accès indirect exercé par un membre de la Commission nationale de l'informatique et des libertés ; que le fichier système d'information Schengen est au nombre des fichiers visés à cet article et que le droit d'accès de M. X ne pouvait être qu'indirect, sans que la Commission nationale de l'informatique et des libertés dispose du droit de communiquer au requérant les informations le concernant contenues dans le fichier ; que M. X n'est, dès lors, pas fondé à soutenir que la Commission nationale de l'informatique et des libertés, en ne lui indiquant pas les informations le concernant contenues dans le fichier système d'information Schengen préalablement au retrait de son signalement, aurait méconnu les dispositions de la loi du 6 janvier 1978 et les stipulations de la convention d'application de l'accord de Schengen ;

Considérant qu'il résulte des dispositions de l'article 38 de la loi du 6 janvier 1978 que l'obligation de notification aux tiers des rectifications opérées sur les informations qui leur ont été transmises, s'impose au responsable du traitement informatisé et non à la Commission nationale de l'informatique et des libertés ; que, dès lors, M. X n'est pas fondé à soutenir que le refus de la Commission nationale de l'informatique de notifier à des tiers les modifications des informations le concernant dans le fichier système d'informations Schengen a méconnu les dispositions de l'article 38 de la loi du 6 janvier 1978 ;

Sur les conclusions à fin d'injonction :

Considérant que la présente décision, qui rejette les conclusions aux fins d'annulation pour excès de pouvoir du requérant, n'appelle aucune mesure d'exécution ; qu'ainsi, ses conclusions à fin d'injonction ne peuvent qu'être rejetées ;

Sur les conclusions de M. X tendant à l'application des dispositions de l'article L. 761 — I du code de justice administrative :

Considérant qu'il n'y a pas lieu, dans les circonstances de l'espèce, de faire application des dispositions de l'article L. 761-1 du code de justice administrative et de condamner l'Etat à payer à M. X la somme qu'il demande au titre des frais exposés par lui et non compris dans les dépens ;

Décide :

Article 1er : il n'y pas lieu de statuer sur les conclusions de M. X dirigées contre la décision implicite de la Commission nationale de l'informatique et des libertés en tant qu'elle refuse de procéder aux modifications des informations le concernant contenues dans le fichier système d'information Schengen.

Article 2 : le surplus des conclusions de M. X est rejeté.

Article 3 : la présente décision sera notifiée à M. Y, à la Commission nationale de l'informatique et des libertés et au garde des Sceaux, ministre de la Justice.

ARRÈT DU CONSEIL D'ÉTAT DU 27 JUILLET 2001
(Req. n° 222509)

Le Conseil d'État statuant au contentieux

Vu la requête, enregistrée le 27 juin 2000 au secrétariat du contentieux, du Conseil d'Etat, présentée par M. X, demeurant... ; M. X demande au Conseil d'Etat l'annulation pour excès de pouvoir de la décision du 21 avril 2000 par laquelle le garde des Sceaux, ministre de la Justice, a refusé d'abroger les arrêtés du 18 juin 1986 et du 13 avril 1993 relatifs à la mise en œuvre dans les tribunaux de grande instance d'un système de gestion automatisé de procédures ;

Vu les autres pièces du dossier ;

Vu la Constitution du 4 octobre 1958 ;

Vu la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel faire à Strasbourg le 28 janvier 1981 et publiée par le décret n° 85-1203 du 15 novembre 1985 ;

Vu le code pénal ;

Vu le code de procédure pénale ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée ;

Vu le code de justice administrative ;

Après avoir entendu en séance publique :

— le rapport de M. Thiellay, maître des requêtes ;
— les conclusions de M. Lamy, commissaire du gouvernement ;

Sur la fin de non-recevoir opposée par le garde des Sceaux :

Considérant que l'autorité compétente, saisie d'une demande tendant à l'abrogation d'un règlement illégal, est tenue d'y déférer, soit que ce règlement ait été illégal dès la date de sa signature, soit que l'illégalité résulte de circonstances de droit ou de fait postérieures à cette date ; que M. X a demandé, le 10 janvier 2000, au garde des Sceaux d'abroger les arrêtés du 18 juin 1986 et du 13 avril 1993 relatifs à la mise en œuvre dans les tribunaux de grande instance d'un système de gestion automatisée de procédures, notamment pénales ; que M. X conteste la légalité de la décision de rejet prise par le garde des Sceaux ; que, par suite, le ministre ne peut utilement soutenir que, les délais de recours pour contester ces arrêtés étant expirés, la requête serait tardive ;

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

Considérant qu'aux termes de l'article 15 de la loi n° 78-17 du 6 janvier 1978 modifiée : « hormis les cas où ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés. / Si l'avis de la Commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'État [...] » ;

Considérant que, saisie par le garde des Sceaux, ministre de la Justice, d'un projet d'arrêté relatif à la mise en œuvre d'un système de gestion automatisée de certaines procédures dans les tribunaux de grande instance, la Commission nationale de l'informatique et des libertés a, par une délibération n° 86-57 du 20 mai 1986, donné un avis favorable à ce projet sous réserve que les informations relatives à la gestion des procédures pénales ne soient pas conservées sur support informatique plus de cinq années à compter du jugement définitif ou de la décision de classement et que les fichiers du greffe soient mis à jour à la suite des mesures d'amnistie, de réhabilitation ou de grâce ; qu'elle a également indiqué que « les informations relatives à la gestion des affaires relevant des attributions non répressives du parquet ne devront pas être conservées, sur support informatique, au-delà du temps nécessaire à l'exercice des contrôles pour lesquels elles ont été enregistrées » ; que le ministre de la Justice a pris, le 18 juin 1986, un arrêté relatif à la mise en œuvre dans les tribunaux de grande instance d'un système de gestion automatisée des procédures pénales et des affaires relevant des procureurs de la République et, le 13 avril 1993, un arrêté relatif à la mise en œuvre d'un système comparable pour les procédures pénales relevant des procureurs de la République et des juges d'instruction, les procédures pénales et civiles des juges des enfants ainsi que les affaires civiles, administratives et commerciales relevant des procureurs de la République ;

Considérant que les conditions posées par la Commission nationale de l'informatique et des libertés pour la création, sur la base de l'article 15 de la loi du 6 janvier 1978, d'un traitement automatisé d'informations nominatives, forment un ensemble destiné à garantir que ce traitement satisfait aux exigences de la loi et assure, de façon satisfaisante, le respect des intérêts que le législateur a entendu protéger ; qu'il en résulte que l'absence, dans l'acte réglementaire de création d'un traitement d'informations nominatives, des mesures propres à assurer le respect des conditions ou réserves figurant dans l'avis préalable de la Commission entache cet acte, dans son ensemble, d'illégalité ; qu'il est constant que les deux arrêtés dont l'abrogation a

été demandée au ministre de la Justice ne prévoient aucune disposition répondant aux conditions fixées par la Commission nationale de l'informatique et des libertés sur les modalités de mise à jour ou de destruction des données faisant l'objet du traitement automatisé ; que, par suite, M. X est fondé à soutenir que les deux arrêtés qu'il conteste, en date, respectivement, du 18 juin 1986 et du 13 avril 1993, sont entachés, dans leur ensemble, d'illégalité et que c'est à tort que le garde des Sceaux a refusé d'en prononcer l'abrogation ;

Considérant toutefois qu'il ressort des pièces du dossier que le traitement automatisé autorisé par les deux arrêtés en cause est nécessaire au bon fonctionnement du service public de la justice ;

Considérant que, dans ces conditions, il y a lieu de décider que le garde des Sceaux disposera d'un délai de deux mois à compter de la notification de la présente décision pour, selon son choix, compléter les arrêtés contestés en prévoyant, conformément à l'avis de la Commission nationale de l'informatique et des libertés du 20 mai 1986, le délai maximal de conservation des données concernant les procédures pénales, c'est-à-dire celles visées aux premier et deuxième tirets de l'article 2 et aux premier, deuxième, troisième, quatrième, septième et huitième tirets de l'article 3, les modalités de mise à jour des informations à la suite des mesures d'amnistie, de réhabilitation et de grâce, ainsi que le délai de conservation des autres informations ou faire prendre un décret, sur avis conforme du Conseil d'Etat, permettant de passer outre les réserves émises par la Commission ;

Considérant que, faute pour le garde des Sceaux d'avoir rétabli, dans le délai fixé ci-dessus, la légalité du traitement automatisé qu'il a autorisé par ses arrêtés des 18 juin 1986 et 13 avril 1993, il devra, sans délai, prononcer l'abrogation desdits arrêtés ;

Décide :

Article 1er : la décision du garde des Sceaux, ministre de la Justice, du 21 avril 2000 refusant d'abroger les arrêtés du 18 juin 1986 et du 13 avril 1993 est annulée. Cette annulation comporte, pour le garde des Sceaux, ministre de la Justice, les obligations exposées dans les motifs de la présente décision qui en constituent le soutien nécessaire.

Article 2 : la présente décision sera notifiée à M. X et au garde des Sceaux, ministre de la Justice.

ARRÈT DU CONSEIL D' ÉTAT DU 30 OCTOBRE 2001 (Req. n° 204909)

Le Conseil d'Etat statuant au contentieux

Vu la requête sommaire et le mémoire complémentaire, enregistrés le 22 février 1999 et le 22 juin 1999 au secrétariat du contentieux du Conseil d'État, présentés pour Association française des sociétés financières et autres, dont le siège social est 24, avenue de la Grande Armée à Paris (75854 Cedex 17), l'Association française des banques, dont le siège social est 18, rue Lafayette à Paris (75440 Cedex 09) et l'Association française des établissements de crédit, dont le siège social est 18, rue Lafayette à Paris (75009) ; l'Association française des sociétés financières et autres, l'association française des banques et l'association française des établissements de crédit demandent au Conseil d'État d'annuler pour excès de pouvoir la délibération n° 98-101 du 22 décembre 1998 de la Commission nationale de l'informatique et des libertés portant modification de la recommandation relative à la

gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit ;

Vu les autres pièces du dossier ;

Vu la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales, notamment son article 6 ;

Vu le traité du 25 mars 1957 instituant la Communauté européenne ;

Vu la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel faite à Strasbourg le 28 janvier 1981 et publiée par le décret n° 85-1203 du 15 novembre 1985 ;

Vu le code pénal ;

Vu la loi n° 78-17 du 6 janvier 1978 ;

Vu le code de justice administrative ;

Après avoir entendu en séance publique :

— le rapport de M. Mochon, maître des requêtes ;

— les observations de la SCP Célice, Blancpain, Soltner, avocat de l'Association française des sociétés financières et autres et autres ;

— les conclusions de M^me^ Maugüé, commissaire du gouvernement ;

Considérant que l'Association française des sociétés financières et autres, l'Association française des banques et l'association française des établissements de crédit défèrent au Conseil d'État la délibération du 22 décembre 1998 par laquelle la Commission nationale de l'informatique et des libertés (CNIL) a entendu modifier sa précédente délibération du 5 juillet 1988 portant adoption d'une recommandation relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit, en lui apportant deux additifs, qui énoncent respectivement, le premier, « que la nationalité » du demandeur « ne peut constituer une variable entrant en ligne de compte dans » le calcul automatisé de l'appréciation du risque, « qu'elle soit considérée sous la forme «Français, ressortissant CEE, autres « ou a *fortiori* enregistrée en tant que telle », et, le second, que « dans le cadre de l'appréciation du risque et au-delà du calcul automatisé qui en est fait, seule la prise en compte de la stabilité de la résidence du demandeur de crédit sur le territoire français constitue une information pertinente » ; que les associations requérantes soutiennent que la Commission nationale de l'informatique et des libertés ne pouvait légalement estimer, comme elle l'a fait, que la prise en compte de la nationalité dans le calcul du « score » destiné à apprécier le risque associé à une demande de crédit ne constituait pas une donnée « adéquate, pertinente et non excessive » au sens de l'article 5 de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel signée à Strasbourg le 28 janvier 1981 ;

Sur *l'exception d'irrecevabilité opposée à la requête par la CNIL :*

Considérant qu'il ressort des termes mêmes de la délibération attaquée, et notamment de son dispositif, qu'elle ne se borne pas à commenter les règles que la CNIL a pour mission de mettre en œuvre, mais qu'elle ajoute à l'ordonnancement juridique ; que les conclusions tendant à son annulation sont par suite recevables ;

Sur la légalité de la délibération attaquée et sans qu'il soit besoin d'examiner les autres moyens de la requête :

Considérant qu'aux termes de l'article 5 de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel signée à Strasbourg le 28 janvier 1981, ratifiée en vertu de la loi du 19 octobre

1982 et publiée au Journal officiel en vertu du décret du 15 novembre 1985 : « les données à caractère personnel faisant l'objet d'un traitement automatisé sont : adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées » ;

Considérant que, pour l'application de ces stipulations, les données pertinentes au regard de la finalité d'un traitement automatisé d'informations nominatives sont celles qui sont en adéquation avec la finalité du traitement et qui sont proportionnées à cette finalité ;

Considérant que le traitement automatisé d'informations nominatives en cause est destiné à aider à la prise des décisions d'octroi ou de refus d'un prêt en contribuant à évaluer le risque qu'une demande présente pour l'établissement prêteur ; qu'il consiste à combiner dans un calcul automatisé divers critères tirés des renseignements que les auteurs de demandes fournissent sur leur situation familiale, professionnelle et bancaire ;

Considérant que la prise en compte de la nationalité d'un demandeur de prêt comme élément d'appréciation d'éventuelles difficultés de recouvrement des créances correspond à la finalité d'un tel traitement ; qu'il ne ressort pas des pièces du dossier relatives aux conditions dans lesquelles cet élément est combiné avec les autres données du calcul automatisé du risque que cette prise en compte soit disproportionnée à son objet ; qu'ainsi c'est à tort que la CNIL s'est fondée sur ce que la nationalité du candidat à un crédit ne constituerait pas une donnée « pertinente, adéquate et non excessive » au regard de la finalité du traitement ;

Considérant, il est vrai, que la CNIL a également entendu se fonder sur les stipulations du traité instituant la Communauté économique européenne prohibant les discriminations fondées sur la nationalité et sur les articles 225-1 et 225-2 du code pénal ;

Mais considérant que la référence à la nationalité comme l'un des éléments de pur fait d'un calcul automatisé du risque, dont la mise en œuvre n'entraîne pas le rejet d'une demande sans l'examen individuel de celle-ci, ne constitue pas une discrimination et dès lors n'entre pas, en tout état de cause, dans le champ d'application de l'article 6 du traité CE, devenu, après modification, l'article 12 CE ; qu'elle ne saurait davantage, en l'absence d'élément intentionnel, être regardée comme tombant sous le coup des articles 225-1 et 225-2 du code pénal ;

Considérant qu'il résulte de ce qui précède que l'Association française des sociétés financières et autres, l'Association française des banques et l'Association française des établissements de crédit sont fondées à demander l'annulation de la délibération n° 98-101 du 22 décembre 1998 de la Commission nationale de l'informatique et des libertés portant modification de la recommandation relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit ;

Décide :

Article 1er : la délibération n° 98-101 du 22 décembre 1998 de la Commission nationale de l'informatique et des libertés portant modification de la recommandation relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit est annulée.

Article 2 : la présente décision sera notifiée à l'Association française des sociétés financières et autres, l'Association française des banques et l'Association française des établissements de crédit, à la Commission nationale de l'informatique et des libertés et au ministre de l'Economie, des Finances et de l'Industrie.

Annexe 7

Actualité parlementaire

Assemblée nationale

Question n^2 : 53997, de M. **Julia Didier,** ministère interrogé : Intérieur
Réponse publiée au JO le : 16 avril 2001 (page 2301)

Droits de l'homme et libertés publiques — Fichiers informatisés. Secret

Question : M. Didier Julia appelle l'attention de M. le ministre de l'Intérieur sur certaines difficultés liées à l'application de la loi informatique et liberté. Ainsi, compte tenu de la pratique fréquente des cessions de fichiers sans accord de l'intéressé, il est impossible de savoir a *priori* qui détient des enregistrements personnels sans en avoir fait la demande auprès de ceux qui pourraient en détenir. Nul ne peut être assuré de connaître tous les traitements sur lesquels il serait inscrit : d'autant plus que la pratique des partages est de plus en plus répandue. En outre, si la CNIL recense tous les fichiers déclarés, il est impossible d'en obtenir une liste compte tenu de leur nombre. En effet, l'énumération des 705 000 déclarations représenterait un listing de plus de quinze kilomètres. Enfin, il n'existe pas d'outil permettant de lister tous les fichiers dans lesquels un nom apparaît. Ainsi, le souci de protection du citoyen caractérisé par l'absence de connexion entre les fichiers est important, mais il peut également nuire à l'accès à ces fichiers, et donc au contrôle que peut avoir la personne visée, ce qui représente une autre atteinte aux libertés. En conséquence, il lui demande s'il envisage des solutions à ces problèmes, et notamment si une révision de la loi informatique et liberté peut être envisagée.

Réponse : la pratique, dénoncée par l'honorable parlementaire, de cessions de fichiers de données personnelles, notamment dans le domaine de la presse, ne permet pas aux personnes concernées de connaître a priori la liste des détenteurs de leurs informations. Pour autant, ces cessions de fichiers ne sont pas nécessairement réalisées en méconnaissance des règles édictées par la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés. En effet, l'article 27 de cette loi impose à tous les responsables de traitements d'informer les personnes auprès desquelles sont recueillies des informations nominatives du caractère obligatoire ou facultatif des réponses, des conséquences à leur égard d'un défaut de réponse, des personnes physiques ou morales destinataires des informations ainsi que de l'existence et des conditions d'exercice de leur droit d'accès et de rectification de ces données. Cette obligation est également applicable lorsque de telles informations sont recueillies par voie de questionnaire. Cependant, chacun a le droit de s'opposer, pour des raisons légitimes et en application de l'article 26 de la loi de 1978, à ce que des informations nominatives le concernant fassent l'objet d'un traitement. C'est donc uniquement parce que ce droit d'opposition n'a pas été exercé en temps utile que la cession des données peut intervenir avec les inconvénients soulignés par l'honorable parlementaire. Il est cependant possible de s'adresser, à tout moment, à chaque organisme avec lequel un contrat ou un abonnement a été souscrit, et qu'il est donc facile d'identifier, pour manifester a *posteriori* son droit d'opposition et demander l'effacement de ses données personnelles dans tous les fichiers des organismes tiers auxquels ces données ont été communiquées par l'organisme qui les a initialement recueilli. La CNIL pourra alors être utilement saisie d'une plainte en cas de non exécution de cette demande et pourra diligenter toutes les investigations nécessaires et contraindre, le cas échéant, l'organisme responsable à exécuter ses obligations d'effacement des données. Il n'apparaît donc pas nécessaire de modifier, sur ce

point précis, la loi de 1978, qui contient déjà les dispositions de nature à répondre aux préoccupations exprimées.

Assemblée nationale

Question n° : 39303 de M. **Rodet Alain,** ministère interrogé : Économie
Réponse publiée au JO le : 07 mai 2001 (page 2706)

Démographie — Recensements. Méthodologie

Question : M. Alain Rodet attire l'attention de M. le ministre de l'Intérieur sur l'inquiétude manifestée par de nombreux élus au sujet de la nouvelle méthode de recensement envisagée par l'INSEE, qui suscite de nombreuses critiques. En effet, le système envisagé ne permettra plus un dénombrement exhaustif de la population (seulement 40 % des logements de communes de plus de 10 000 habitants seront recensés). De plus, les données collectées la première année ne correspondront plus à la réalité cinq ans plus tard, compte tenu de la mobilité de la population. On peut également craindre un désintérêt des habitants, faute de campagne de communication nationale. Les élus locaux déplorent aussi le choix de quadrillage fait par l'INSEE, trop restrictif et ne permettant pas une vision globale des zones recensées. Enfin, l'incidence de ce projet sur le budget communal est préoccupante : en effet, aux frais de recrutement de nouveaux agents recenseurs chaque année, s'ajouteront les coûts liés à l'acquisition des renseignements collectés auprès de l'INSEE qui, par le biais d'accès payants aux données ou d'abonnements, revendra ainsi aux communes des informations dont elles auront elles-mêmes financé la collecte. En conséquence, il lui demande quelles mesures le Gouvernement compte prendre pour répondre à ces inquiétudes.

Réponse : l'Institut national de la statistique et des études économiques étudie une nouvelle méthode de recensement qui sera présentée au Parlement à l'occasion d'un futur projet de loi portant diverses dispositions d'ordre économique et financier. Celle-ci, chaque année, s'appuierait sur une collecte d'information auprès de la population, réalisée par sondage, complétée par des données statistiques tirées des sources administratives. Dans les communes de 10 000 habitants ou plus, cette opération se ferait de façon tournante, l'ensemble des immeubles de la commune étant réparti en cinq groupes. Chaque année, le recueil des informations serait fait auprès d'un de ces groupes d'immeubles. Il serait réalisé en deux temps : un repérage de tous les logements, suivi d'une collecte d'information sur une partie de ces logements et sur leurs occupants. Le recours au sondage à partir de tous les logements des immeubles observés une année donnée permettant d'atteindre un meilleur taux de réponse, le taux de sondage (40 %) et l'utilisation statistique de sources administratives assureront une bonne précision de la population légale. Les communes de moins de 10 000 habitants seraient recensées exhaustivement, à raison d'une sur cinq chaque année. Pour obtenir des données annuelles, l'actualisation entre deux collectes se ferait à partir des sources administratives. L'apport principal de la rénovation est donc l'actualité des données, essentielle dans une société soumise à des changements rapides. Mieux qu'un recensement ponctuel réalisé tous les sept à neuf ans, elle permettra de suivre les évolutions récentes. En effet, chaque année environ 10 % des individus déménagent, dont 6,5 % avec changement de commune. Une telle méthode où tous les habitants ne sont pas concernés au même moment par les opérations de collecte appellera une campagne de communication appropriée. Celle-ci comportera nécessairement un volet local, toutes les communes n'étant pas impliquées chaque année dans la collecte. Dans les grandes communes, il faudra

pouvoir répondre à la question « Pourquoi suis-je recensé et pas mon voisin ? ». La campagne locale de communication serait conçue et testée en lien avec les associations d'élus et rappellerait les enjeux du recensement pour assurer la mobilisation des habitants. Un module sera développé pour expliquer l'importance de répondre même à un sondage. La formation donnée aux agents recenseurs intégrera un argumentaire en réponse à cette question. Pour la diffusion, il est envisagé une diffusion standard selon un découpage par quartier d'environ 2 000 habitants (découpage IRIS 2000). Comme pour le recensement de la population de 1999, et sous réserve de l'avis de la Commission nationale de l'informatique et des libertés, les communes pourront obtenir des données sur des zones plus fines. Concernant le coût d'accès aux données, l'expérience montre que celui-ci diminue fortement avec l'utilisation des nouvelles technologies. Cela a d'ailleurs été le cas entre les recensements de 1990 et 1999. La procédure nouvelle ne devrait donc pas induire un coût accru pour les collectivités locales. Au contraire, à terme, le recensement nécessitera des besoins matériels réduits, coordonné à la gestion courante et donc intégré de manière naturelle à l'activité de la commune. Dans les grandes villes en particulier, la diminution des charges une année donnée supprimera la nécessité d'une logistique spécifique. Dès lors, comme dans la procédure actuelle, l'État verserait aux communes une dotation forfaitaire fonction de critères simples.

Sénat

Question n^{5} : 32587 de M. **Hamel Emmanuel,** ministère de dépôt : Santé
Réponse publiée au JO le : **19 juillet 2001** (page : 2397)

Manque de transparence des sites de santé sur Internet

Question : M. Emmanuel Hamel attire l'attention de M. le ministre délégué à la Santé sur l'information parue à la page 12 du quotidien *Le Figaro* du 16 mars 2001 selon laquelle la Commission nationale informatique et libertés déplore le manque de transparence des sites de santé sur Internet et « estime que la confidentialité des données n'est pas assurée ». Il souhaiterait connaître son avis sur les conclusions de cette étude et les mesures envisagées par le Gouvernement pour remédier à cette situation.

Réponse : les sites Internet consacrés à la santé se multiplient. De nombreux services médicaux virtuels sont aujourd'hui proposés à destination du grand public : publication d'informations médicales, avis médicaux en ligne, gestion de données personnelles de santé, etc. Le constat partagé par tous les acteurs est que le domaine particulier de la e-santé, compte tenu des risques pour l'usager, se développe avec une trop grande hétérogénéité dans la qualité des informations et des services proposés. Or, pour l'internaute, il n'existe pas de repère clair lui permettant de juger de la qualité de ce qu'il consulte ou des services qu'il utilise. Le ministère chargé de la Santé en collaboration avec les ordres professionnels et plus particulièrement avec l'Ordre national des médecins, a lancé le projet « qualité des sites e-santé » dès le printemps 2000. Ce projet a notamment pour objectif de dégager un référentiel de qualité qui permettra à l'internaute de se faire lui-même une opinion sur la qualité des sites Internet qu'il consulte et d'assurer à l'usager que les sites qui se réclament de ces règles les respectent bien. Par ailleurs, et conformément à la recommandation de la CNIL, un article de loi visant à mettre en place un dispositif d'autorisation préalable des personnes dépositaires de données de santé à caractère personnel est actuellement à l'étude et devrait pouvoir prendre place dans un futur projet de loi. Cette autorisation aura pour objectif de s'assurer que toutes les

dispositions ont été prises pour préserver la confidentialité et la sécurité des données traitées.

Sénat

Question n^{e} : 34256, de M. **Trégouët René,** ministère de dépôt : Affaires européennes Réponse publiée *au JO* le : 09 août 2001 (page : 2599)

Intégrité des données informatiques personnelles

Question : M. René Trégouët rappelle à l'attention de M. le ministre délégué chargé des Affaires européennes les déclarations faites fin juin dernier par un responsable américain du commerce extérieur invitant l'Union européenne à rechercher une alternative au modèle de contrat récemment adopté par les États membres pour garantir l'intégrité des données informatiques personnelles envoyées vers des pays extérieurs. Les options permises par ce modèle sont selon lui trop limitées. Une telle invitation est-elle envisageable pour le gouvernement français ?

Réponse : l'honorable parlementaire a bien voulu appeler l'attention du ministre délégué chargé des affaires européennes sur les déclarations faites en juin dernier par un responsable américain du commerce extérieur invitant l'Union européenne à rechercher une alternative au modèle de contrat récemment adopté par les États membres pour garantir l'intégrité des données informatiques personnelles envoyées vers des pays extérieurs, les options permises par ce modèle étant selon lui trop limitées. L'hypothèse d'une possible évolution de ce type de contrat doit être replacée dans le contexte de l'accord entre l'Union européenne et les États-Unis sur la question de la protection des données personnelles. La directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit en effet un régime très protecteur des individus pour les données collectées, traitées et utilisées à l'intérieur de l'Union. Elle prévoit, en outre, le cas des transferts de données à caractère personnel collectées dans l'Union vers des pays tiers. Aux termes de l'article 25, le transfert ne peut avoir lieu que si « le pays tiers en question assure un niveau de protection adéquat » (qui n'implique d'ailleurs pas une protection « équivalente » à celle offerte par la directive aux transferts de données entre États membres de l'Union). Lorsque ce niveau de protection n'est pas atteint, la Commission peut alors engager des négociations avec lui en vue de remédier à la situation (article 25-5). C'est en vertu de ces dispositions que la Commission a engagé une négociation avec les États-Unis. En effet, ceux-ci s'en remettent davantage à l'autorégulation du secteur pour la protection de la vie privée. Ce cadre juridique plus « laxiste », dans le contexte de la société de l'information, a pu favoriser le développement d'un commerce lucratif, non toujours exempt de dérives : exploitation de fichiers de sécurité sociale par des compagnies d'assurance ; des fichiers de cartes de crédit (avec le détail des opérations) par des sociétés de marketing, etc. Cette dérive commerciale est fortement aggravée par le développement d'Internet qui facilite le recoupement de fichiers et la construction de banques de données personnelles, à partir d'informations collectées sur la toile par de puissants moteurs de recherche. La *Federal Trade Commission* a d'ailleurs publié un rapport constatant l'insuffisance des mécanismes d'autorégulation en matière de protection de la vie privée sur Internet et recommandant au congrès l'élaboration d'une nouvelle législation plus protectrice. Afin de concilier leurs logiques juridiques contraires, l'Union européenne et les États-Unis se sont accordés en juin 2000 sur un mécanisme de *« safe harbors »* (zo-

nes sécurisées). Ce système prévoit l'édiction d'un code de conduite — sous forme de « principes de respect de la vie privée » — par le département américain du commerce. Les entreprises qui souscrivent à ce code, sur une base volontaire, sont enregistrées auprès d'un certain nombre d'organismes privés indépendants. Cet enregistrement vaut habilitation à traiter des données personnelles en provenance de l'Union européenne. L'ensemble du système est placé sous le contrôle de la *Federal Trade Commission* qui dispose de pouvoirs de sanction administrative et peut engager une action devant les tribunaux américains contre une entreprise qui n'aurait pas respecté ses engagements contractuels au titre des safe harbors. Ce mécanisme — auquel a adhéré récemment une société aussi importante que Microsoft — est désormais opérationnel. Les clauses contractuelles types auxquelles fait allusion le responsable américain du commerce cité par l'honorable parlementaire sont celles prévues à l'article 26-4 de la directive 95/46. Elles permettent les transferts de données interentreprises vers tout pays tiers n'offrant pas un niveau de protection adéquat. S'agissant des États-Unis, elles permettent les transferts de données vers des entreprises n'adhérant pas au système du safe *harbor.* Si des entreprises déplorent que les options permises par ce modèle sont très limitées, en réalité, rien ne les empêche d'adhérer à une plate-forme sécurisée.

Assemblée nationale

Question n° : 61143, de M. **Adevah-Pœuf Maurice,** ministère de dépôt : Ville
Réponse publiée au JO le : 13 août 2001 (page : 4735)

Logement — HLM. Conditions d'attribution. Personnes surendettées

Question : M. Maurice Adevah-Pœuf attire l'attention de M. le ministre délégué à la Ville sur une pratique de certains organismes d'HLM publics ou privés, notamment dans le Puy-de-Dôme. En effet, le questionnaire remis aux candidats à un logement social comporterait une rubrique exigeant que le demandeur précise s'il fait l'objet d'un plan d'apurement de ses dettes dans le cadre de la loi sur le surendettement. Si un tel plan existe, l'organisme HLM demande copie détaillée de ce dernier. Si l'existence d'un tel plan ne justifie pas formellement le refus d'un logement, il semblerait néanmoins que les demandeurs, inscrits dans une procédure de surendettement, aient des difficultés particulières pour obtenir un logement. Si de telles pratiques se révélaient exactes, elles contreviendraient à la volonté du législateur, qui, s'est exprimée dans la loi contre les exclusions et dans les textes relatifs au logement. Elles seraient également en infraction avec le secret professionnel relatif à la procédure du surendettement et avec la loi relative à l'informatique, aux fichiers et aux libertés. De plus, de telles pratiques mettent à mal les recommandations de la commission d'examen des situations de surendettement qui incitent souvent le demandeur à trouver des solutions de logement moins onéreuses. Il est particulièrement choquant que des bailleurs sociaux, qui devraient être en première ligne dans la lutte contre les exclusions, participent à aggraver la situation de familles en difficulté. Aussi, il lui demande de bien vouloir lui faire part de sa position sur ce sujet et de lui indiquer les dispositions qu'elle entend mettre en œuvre pour remédier à ces pratiques.

Réponse : l'honorable parlementaire attire l'attention du ministre délégué à la Ville sur une pratique de bailleurs sociaux consistant à demander aux candidats à un logement social une déclaration sur l'honneur précisant s'ils ont fait l'objet d'un plan d'apurement de leurs dettes en commission de surendettement et, le cas échéant, copie du plan d'apurement. De telles pratiques conduiraient à exclure certaines familles des procédures d'attribution de logements sociaux. S'agissant des élé-

ments à fournir à l'appui d'une demande de logement, il n'existe actuellement aucune disposition législative ou réglementaire qui définisse la totalité des pièces ou éléments d'information qui peuvent être exigés du candidat locataire par le bailleur. Toutefois, la demande d'information des organismes HLM doit se limiter aux seuls éléments nécessaires pour apprécier la recevabilité des candidatures à l'attribution d'un logement. Conformément à l'article L. 441-1 du code de la construction et de l'habitation, pour l'attribution des logements locatifs sociaux, il est notamment tenu compte du niveau de ressources des ménages. Aussi peut-on considérer que l'existence d'un plan de redressement établi par une commission de surendettement, en application de l'article L. 331-6 du code de la consommation, est un élément qui peut être utile au bailleur pour s'assurer de la solvabilité des candidats et rechercher s'il y a lieu une solution de logement adaptée à leurs ressources (logement adapté, aide du fonds de solidarité pour le logement...). En outre, une telle précaution peut également s'avérer utile pour le candidat au logement dont l'inadaptation des ressources ne lui permettrait pas d'acquitter le loyer et les charges correspondants et pourrait ainsi aggraver son endettement. L'appréciation économique du taux d'effort attendu du ménage peut cependant varier d'un département à l'autre. À cet égard, le ministre délégué à la Ville entend engager avec la secrétaire d'Etat au logement une réflexion sur une harmonisation possible des règlements financiers des FSL. Au-delà de la connaissance de l'existence d'un plan de redressement, l'honorable parlementaire a tout à fait raison de souligner que les bailleurs sociaux ne peuvent exiger du candidat locataire la copie du plan de redressement établi par une commission de surendettement. Cela ressort clairement des dispositions de l'article L. 333-4 du code de la consommation. L'accès à ces informations est limité à la Banque de France, aux établissements de crédit et aux services financiers de La Poste. S'agissant de la régularité des pratiques relevées par l'honorable parlementaire au regard de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il convient de distinguer les informations exigées des candidats locataires pour la constitution de leur dossier, des informations faisant l'objet d'une gestion par le biais d'un fichier. Dans le second cas, la loi prévoit que les traitements automatisés d'informations nominatives, opérés notamment pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés (CNIL). En l'espèce, il ne s'agit *a priori* que de la constitution de dossiers de demande de logement en vue de leur examen par les commissions d'attribution. S'il s'avérait néanmoins que l'existence d'un plan de redressement établi en commission de surendettement était mentionnée dans les fichiers de gestion des bailleurs sociaux, ceux-ci devraient se mettre en conformité avec la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Assemblée nationale

Question n° : 60393, de M. **Muselier Renaud,** ministère de dépôt : Intérieur
Réponse publiée au JO le : 13 août 2001 (page: 4715)

Droit pénal — Agressions sexuelles. Fichier génétique. Création. Délais

Question : M. Renaud Muselier appelle l'attention de M. le ministre de l'Intérieur sur les délais de mise en place du fichier national automatisé des empreintes génétiques (FNAEG). Voté au Parlement le 17 juin 1998, ce dernier n'a pas encore vu le jour à l'heure qu'il est. Il constituerait pourtant un outil remarquable d'identification des criminels et permettrait à l'évidence de prévenir nombre d'ac-

fions criminelles en identifiant plus rapidement leurs auteurs. Avec un risque d'erreurs tellement minime (les scientifiques estiment la possibilité de trouver un même profil génétique à un sur 700 000 milliards), il ouvre des perspectives intéressantes à la justice et à la sécurité des personnes, qui se doivent d'être exploitées au plus vite. En conséquence, il souhaite connaître son sentiment sur cette question et savoir quelles échéances sont envisageables pour son installation opérationnelle.

Réponse : à la différence des autres grands fichiers publics, pour lesquels la saisine de la Commission nationale de l'informatique et des libertés n'intervient qu'après la réalisation des développements informatiques indispensables pour tester le fonctionnement du projet, la création du fichier national automatisé des empreintes génétiques (FNAEG), par la loi du 17 juin 1998, n'a été précédée d'aucune étude sur le plan technique. Ces études ont donc dû être conduites après le vote de la loi et parallèlement à l'élaboration du décret n° 2000-413 du 18 mai 2000, qui a défini les conditions d'application des dispositions de la loi sur le FNAEG, dans le respect des prescriptions préconisées successivement par la CNIL et par le Conseil d'État, en matière de protection des données à caractère personnel, et de l'arrêté du 18 mai 2000, fixant la liste des segments d'ADN sur lesquels portent les analyses génétiques pratiquées aux fins d'utilisation du FNAEG. Un groupe du travail police-gendar merie, constitué sous la présidence d'un magistrat du bureau de la police judiciaire de la chancellerie, s'est réuni à plusieurs reprises afin de traiter des problèmes juridi ques induits par ce fichier, et la chancellerie a diffusé le 10 octobre 2000 une circu laire aux parquets présentant le fichier afin de préparer son alimentation. De même, la garde des Sceaux a désigné, par un arrêté au 2 avril 2001, le magistrat hors hié rarchie chargé, aux termes de l'article R. 53-16 du code de procédure pénale, d'as surer le contrôle du FNAEG. Par ailleurs, les trois personnes qualifiées en génétique et/ou en informatique, chargées aux termes de ce même article, d'assister ce magis trat dans sa mission de contrôle du FNAEG ont été désignées par arrêté du 15 juin 2001. Sur le plan matériel, des locaux ont été spécialement aménagés à Ecully par la sous-direction de la police technique et scientifique qui a également procédé au re crutement des personnels nécessaires et à l'acquisition des équipements informati ques. Des équipements complémentaires destinés à renforcer la sécurité des locaux sont en cours de réalisation. Le système pourra commencer à fonctionner dès juillet 2001 pour une mise en service opérationnelle fin 2001 et une mise en œuvre de fonctionnalités périphériques et secondaires dans une version stable et définitive (hors stockage final) à l'été 2002.

Assemblée nationale

Question n° : 22894, de M. **Hage Georges,** ministère de dépôt : Premier ministre
Ministère attributaire : Intérieur
Réponse publiée au JO le : 27 août 2001 (page : 4937)

Police judiciaire — Fichier. Création. Débat au Parlement

Question : M. Georges Hage attire l'attention de M. le Premier ministre sur l'émotion suscitée par la mise en oeuvre du système de traitement informatique criminel (STIC) détenu par le ministère de l'Intérieur français. Le STIC conduit, en dehors de toutes règles posées par le code de procédure pénale, à faire le procès non contradictoire, secret et obscur, des origines par une extraction massive et systématique des données relatives à chaque individu tendant à figer les situations. Le but du STIC n'est pas la mission de police judiciaire mais de police administrative, de police de l'information, visant à opérer des enquêtes d'honorabilité qui constituent une atteinte

à la vie privée. Le STIC, sans contrôle et sans règle, serait une atteinte directe aux garanties fondamentales dont doivent bénéficier tout citoyen et une tentative choquante de la réduction des droits de la défense et de la présomption d'innocence. Le ministère de l'intérieur n'a prévu aucun mécanisme de contrôle et d'actualisation du fichier par le ministère de la justice. L'État de droit a pour fin essentielle les garanties et la protection fondamentales de la personne. Les organes de l'État de droit, c'est-à-dire notamment la police, doivent donc, eux aussi, être ordonnés à cette fin. En l'espèce, aucune procédure n'a été mise en place pour que les données nominatives enregistrées dans le STIC soient actualisées au vu et au su des suites judiciaires données à l'enquête policière. Autrement dit, une personne ayant bénéficié d'une décision judiciaire de non-lieu, de relaxe ou d'acquittement, reste fichée, pour un temps indéterminé, en tant que « connue par les services de police comme auteur ou coauteur » de faits délictueux. Plus grave, de simples témoins entendus par les services de police se verront fichés sans distinction à côté de délinquants ou criminels, comme impliqués dans une affaire délictueuse. En l'espèce, le simple avis de la CNIL ne peut se substituer à un vote du Parlement. Il s'agit d'une question trop grave pour qu'elle s'opère en dehors d'un débat sur la place publique au sein des institutions représentatives nationales (Assemblée nationale, Sénat) et communautaire (Parlement européen). Il lui demande quelles mesures il compte prendre pour que les libertés individuelles soient effectivement garanties.

Réponse : le système de traitement des infractions constatées (STIC) est un fichier de police judiciaire dont la finalité est la rationalisation du recueil et de l'exploitation des informations contenues dans les procédures établies par les services de police, dans le cadre de leur mission de police judiciaire, aux fins de recherches criminelles et de statistiques. Ce fichier a été autorisé par décret n° 2001-583 du 5 juillet 2001 pris sur avis conforme de la CNIL, en date du 19 décembre 2000, et sur avis favorable du Conseil d'État du 19 février 2001. Ce décret a été publié au *Journal officiel* du 6 juillet 2001. Placé sous le contrôle du procureur de la République et de la CNIL, le STIC est constitué des informations recueillies dans les comptes rendus d'enquête rédigés à partir des procédures établies par les services de police, dans le cadre de leur mission de police judiciaire, lorsqu'elles concernent des personnes à l'encontre desquelles sont réunis, fors de l'enquête préliminaire, de l'enquête de flagrance ou sur commission rogatoire, des indices ou des éléments graves et concordants attestant leur participation à la commission d'un crime, d'un délit ou d'une contravention de cinquième classe prévue aux articles R. 625-1, R. *625-7,* R. 625-8, R. 635-1, R. 645-1 et R. 645-12 du code pénal, ou les victimes de ces infractions.

Assemblée nationale

Question n° : 64435, de M. **Braouezec Patrick,** ministère interrogé : Justice
Réponse publiée au JO le : 03 septembre 2001 (page : 5089)

Conseils de prud'hommes —Jugements. Fichiers informatisés. Accès

Question : M. Patrick Braouezec appelle l'attention de M^{me} la garde des Sceaux, ministre de la justice, sur la conservation informatisée et la communicabilité des jugements auprès des conseils de prud'hommes. Le principe de la communicabilité de ces pièces, qui comportent des données personnelles, découle du caractère public des audiences. Au demeurant/sous peine d'être attentatoire aux libertés, notamment syndicales, ce principe doit s'exercer sur la base d'une demande et de références précises et non sur celle de l'utilisation de fichiers informatisés, qui constitue-

raient une sorte de « casier prud'homal » des individus. Des cas d'espèce font apparaître que des employeurs ont eu accès à ces données sur la base de la seule identité d'une personne et ont pu en user à l'endroit d'un salarié ou d'un candidat. Nombre de conseils de prud'hommes ont aujourd'hui constitué des fichiers informatisés. Il convient de s'interroger sur l'opportunité même de tels fichiers et de mettre en regard la rationalisation du travail qu'ils permettent et les risques de dérapages qu'ils comportent. De même, il apparaît nécessaire d'une part de préciser que le délai de conservation informatique de ces données est bien d'une année, et d'autre part de fixer le point de départ à ce délai d'un an. Les pratiques observées varient de la date du dépôt de plainte jusqu'à celle du résultat du jugement en appel. Aussi, il souhaite connaître les moyens de contrôle qu'elle peut mettre en œuvre afin de garantir une meilleure protection de ces données, tant au travers de ses services qu'au travers d'une mission confiée à la Commission nationale informatique et libertés.

Réponse : la garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que la conservation informatisée et la communicabilité des jugements auprès des conseils de prud'hommes sont effectuées selon les principes de sécurité suivants et le respect des mesures légales énoncées ci-après. L'arrêté du 20 juilletl 994 (*JO* du 4 août 1994) a autorisé la gestion automatisée des affaires relevant de la compétence des conseils de prud'hommes. L'article 5 détermine la liste des destinataires de ces informations : s'agissant des informations relatives aux procédures en cours, les magistrats, conseillers et fonctionnaires du greffe ainsi que le ministre de la Justice ; s'agissant de la gestion des personnels et de la comptabilité, les fonctionnaires du greffe et le ministère de la Justice. L'article 9 donne obligation à toute juridiction concernée de procéder à une déclaration conforme au modèle type et de préciser les mesures de sécurité et de confidentialité, tant physiques que logiques adoptées. Les conseils de prud'hommes utilisent les progiciels relevant de la propriété du ministère pour la gestion des affaires de leur compétence, dans le respect des consignes édictées par l'arrêté sus-visé. Aussi le greffier en chef, chef de greffe du conseil de prud'hommes, doit-il s'assurer qu'aucune information ne soit divulguée à des tiers. Par ailleurs, l'article 11-3 de la loi n° 72-626 du 5 juillet 1972 modifiée dispose que « les tiers sont en droit de se faire délivrer copie des jugements prononcés publiquement ». Cette délivrance n'est plus soumise à droit de timbre depuis l'entrée en vigueur de la loi de finances pour 2000 (article 31 de la loi n° 99-1172 du 30 décembre 1999). La délivrance des copies de décisions aux tiers ne peut intervenir que sur fourniture d'indications précises des décisions sollicitées (date de l'audience et identité des parties) : la personne en charge de la conservation des minutes et des décisions de justice (le greffier en chef, chef de greffe du conseil de prud'hommes selon l'article R. 831-1 du code de l'organisation judiciaire) délivrera copie de la décision demandée. Un refus de délivrance peut d'ailleurs intervenir, notamment en cas de demande qui pourrait paraître abusive. L'article 1441 du nouveau code de procédure civile organise les voies de recours contre une telle décision. Enfin le progiciel de gestion des affaires relevant de la compétence des conseils de prud'hommes comporte un module d'archivage. Celui-ci est utilisé par le greffier en chef, chef de greffe de la juridiction. Il s'assure également que les décisions ne soient conservées que dans le strict respect des délais de l'article 7 de l'arrêté du 20 juillet 1994 (un an à compter de la date à laquelle la décision est devenue définitive). Les intéressés ont la possibilité de vérifier le respect de cette conservation et de formuler éventuellement une requête à la Commission nationale informatique et libertés si celle-ci n'était pas respectée. Le ministère de la Justice est destinataire des réclamations opérées par les personnes et veille au bon respect de ces dispositions.

Assemblée nationale

Question n° : 60995, de M^me^ **Bachelot-Narquin Roselyne,** ministère interrogé : Économie
Réponse publiée au JO le : 10 septembre 2001 (page : 5178)

Banques et établissements financiers — Prêts. Conditions d'attribution

Question : M^me^ Roselyne Bachelot-Narquin appelle l'attention de M. le ministre de l'Économie, des Finances et de l'Industrie sur le problème du fichage à la Banque de France des gérants d'entreprises ayant dû déposer leur bilan. Même si ce dépôt de bilan remonte à des années et que la personne concernée a, entre-temps, réussi à bâtir une affaire florissante, ce fichage perdure, entretenant ainsi la suspicion et surtout l*a* réticence, notamment des banquiers. L'obtention d'un crédit dans de telles conditions ne se fait pas sans d'extrêmes difficultés, alors qu'il paraîtrait plus légitime que la banque statue sur la situation présente de l'entreprise, et non sur un ancien dépôt de bilan. Elle lui demande quelles mesures il entend prendre à ce sujet, car de tels procédés ne contribuent pas à encourager la création d'entreprises et la prise de risque et d'initiative dans le domaine économique.

Réponse : la base de données nationale intitulée « fichier bancaire des entreprises » (FIBEN), tenue par la Banque de France, enregistre des informations concernant les entreprises industrielles et commerciales et leurs dirigeants. Ces informations ne peuvent être communiquées qu'aux établissements de crédit et à quelques administrations à vocation économique qui interrogent la Banque de France. Ce fichier, en application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, a reçu un avis favorable de la Commission nationale de l'informatique et des libertés par délibération n° 87-69 du 7 juillet 1987. La base de données FIBEN diffuse notamment la cotation attribuée par la Banque de France aux entreprises et à leurs dirigeants. Il est vrai que la Banque de France est, le plus souvent, amenée à attribuer une cote réservée aux dirigeants d'entreprise qui ont fait l'objet d'une procédure collective. Cette cote *est* donc fondée sur le fait objectif qu'ils ont été à la tête d'entreprises ayant rencontré des difficultés financières. La cotation Banque de France constitue une cote purement informative qui ne peut être assimilée à une cote « sanction ». Il en résulte que les établissements de crédit qui, au demeurant, n'ont pas l'obligation de consulter FIBEN, sont libres de ne pas tenir compte de l'appréciation émise par la Banque de France dans leurs rapports commerciaux avec leurs clients. Ainsi, les établissements de crédit demeurent libres de consentir ou non un concours à des personnes dont la cote est défavorable. L'établissement prêteur dispose en effet de sa propre grille d'analyse et peut faire usage de multiples sources de renseignements (Infogreffe, Greftel, INPI, sociétés privées de renseignements) avant de prendre sa décision d'octroi ou de refus. La Commission nationale de l'informatique et des libertés, dans sa délibération n° 96-060 du 9 juillet 1996, a observé que « la cotation attribuée à un dirigeant était un signal devant permettre, en cas de réserve, le déclenchement d'investigations plus approfondies par les établissements de crédit ». La loi du 6 janvier 1978 n'impose l'information des personnes fichées que lorsque les renseignements enregistrés sont directement recueillis auprès de ces personnes. Cette interprétation a été confirmée par la chambre criminelle de la Cour de cassation en octobre 1995. Au demeurant, en accord *avec* la Commission nationale de l'informatique et des libertés, la Banque de France a décidé d'informer, de façon systématique depuis le 1^er^ janvier 1997, les dirigeants et entrepreneurs individuels auxquels elle attribue une cote réservée. En outre, dans l'attribution de la cotation, il n'est tenu compte que des informations que la Banque de France est légalement autorisée à enregistrer, ce qui exclut les décisions judiciaires

de nature commerciale visées par les lois portant amnistie ainsi que les condamnations en rapport avec une procédure pénale. Pour les sociétés de capitaux, il n'est tenu compte des liquidations judiciaires que pendant les cinq années suivant la décision judiciaire. Enfin, les représentants légaux d'une entreprise bénéficient d'un droit d'accès et de rectification des informations détenues à leurs noms par la Banque de France dans la base de données FIBEN, conformément aux dispositions de cette loi.

Assemblée nationale

Question n° : 64824, de M. de **Chazeaux Olivier,** ministère de dépôt : Intérieur
Réponse publiée au JO le : 17 septembre 2001 page : 5357

Sous-préfectures — Informations concernant les associations. Communication

Question : certaines sous-préfectures, invoquant une délibération de la CNIL du 16 juin 1987 et un arrêté ministériel du 22 septembre 1987, refusent d'assurer la publicité prévue par la loi du 1er juillet 1901 sur les associations, à savoir la communication au public de l'identité et du domicile des dirigeants tels qu'ils figurent dans les déclarations qui leur sont faites. Il semblerait qu'il existe des divergences d'interprétation de ces deux textes, car la plupart des sous-préfectures continuent d'appliquer les dispositions de la loi de 1901 sur la publicité des associations. Par ailleurs, d'autres sous-préfectures acceptent que le public consulte cette liste sur place, mais refusent d'en délivrer une copie et ce, bien que l'article 2 du décret du 16 août 1901 stipule expressément que toute personne peut se faire délivrer, à ses frais, des extraits de statuts et de déclarations. Bien que les sous-préfectures concernées soient en nombre limité, cette absence de transparence peut être susceptible de favoriser de graves dérives dans la gestion de certaines associations. Aussi, M. Olivier de Chazeaux demande à M. le ministre de l'Intérieur de bien vouloir lui confirmer cette règle de droit à savoir, que l'identité et le domicile des dirigeants d'une association doivent être communiqués à toute personne qui en fait la demande, soit sur place, soit par courrier, moyennant frais de photocopie et d'envoi à sa charge.

Réponse : aux termes des dispositions prévues à l'article 2 du décret du 16 août 1901, « toute personne a droit de prendre communication sans déplacement, au secrétariat de la préfecture ou de la sous-préfecture, des statuts et déclarations ainsi que des pièces faisant connaître les modifications de statuts et les changements survenus dans l'administration ou la direction. Elle peut même s'en faire délivrer à ses frais expédition ou extrait ». Aux termes de l'article 5 de la loi du 1er juillet 1901 modifiée, la déclaration préalable fait connaître «le titre et l'objet de l'association, le siège de ses établissements et les noms et professions, domiciles et nationalités de ceux qui, à un titre quelconque, sont chargés de son administration ou de sa direction ». L'exercice de ce droit d'accès pour toute personne qui en fait la demande a été confirmé par le Conseil d'État dans ses *arrêts Clément des 5* juillet 1993 et 17 janvier 1994. La haute assemblée a précisé à cette occasion que la communication de la date et du lieu de naissance des dirigeants d'associations n'entrait pas dans la liste des éléments communicables aux tiers, dès lors qu'ils ne figurent pas au nombre des renseignements énumérés par les textes précités.

Sénat

Question n[2] : 31421, de M. **Bohl André,** ministère interrogé : Premier ministre
Réponse publiée au JO le : 20 septembre 2001 (page : 3029]

Transposition de la directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Question : M. André Bohl appelle l'attention de M. le Premier ministre sur le retard pris dans la saisine du Parlement de la transposition de la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Ce texte doit procéder à l'adaptation de loi n° 78-17 du 6 janvier 1978. Il doit permettre à la Commission nationale informatique et libertés la saisi ne des risques particuliers au regard des droits et libertés du fait des traitements mis en place par des organismes du secteur privé. L'informatique a des développements tels dans le secteur privé que le cantonnement du contrôle de la mise en oeuvre des traitements au secteur public est insuffisant pour protéger les libertés des personnes dans un monde où les échanges de données ne peuvent pas être limités au territoire national. Il serait heureux que ce texte puisse être déposé au moment où la France accueille la XXIII[e] Conférence internationale des organismes de protection des personnes en septembre. Le dépôt de ce projet de loi avait été expressément prévu lors de l'examen du projet de loi autorisant le Gouvernement à transposer par ordonnances diverses directives. Ce texte ayant été approuvé par le Parlement et promulgué, il demande quand le Gouvernement entend mettre en oeuvre les moyens pour transposer en droit français la directive précitée.

Réponse : l'honorable parlementaire attire l'attention de M, le Premier ministre sur la transposition de la directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. M. le Premier ministre précise que ce projet de loi a été présenté lors du conseil des ministres du 18 juillet 2001, en vue de son examen par le Parlement.

Assemblée nationale

Question n° : 63438 de M. **Deflesselles Bernard,** ministère interrogé : Justice
Réponse publiée au JO le : 15 octobre 2001 (page : 5965)

Droit pénal — Agressions sexuelles. Fichier génétique

Question : M. Bernard Deflesselles attire l'attention de M[me] la garde des Sceaux, ministre de la Justice, sur la mise en place du fichier national d'empreintes génétiques. Les empreintes génétiques par prélèvement d'ADN constituent une véritable « carte d'identité biologique » dont l'usage en matière judiciaire a marqué une véritable révolution. Aujourd'hui, de nombreuses affaires sont élucidées par la comparaison de l'ADN retrouvée sur les victimes avec celui de délinquants déjà connus. L'efficacité de ces procédures est stupéfiante tant pour identifier les criminels que pour innocenter des personnes soupçonnées à tort. Après l'adoption de la loi du 17 juin *1*998 créant un fichier national d'empreintes génétiques et la publication tardive du décret de mai 2000 qui en a précisé les modalités d'application, il est temps d'entrer dans la phase concrète de la constitution de ce fichier dont les débuts s'avèrent difficiles. Ce fichier sera d'une faible efficacité puisque n'y figureront que les empreintes génétiques des personnes condamnées et ayant épuisé toutes les voies de recours. Autant dire que le personnel judiciaire ne disposera d'un fichier que dans

plusieurs années, ne contenant que des empreintes génétiques de quelques auteurs de crimes condamnés à vie. Par conséquent, ce fichier ne permettra jamais une comparaison effective des empreintes relevées sur les nouvelles victimes. De surcroît, les laboratoires habilités à effectuer les recherches d'ADN n'utilisent pas tous les mêmes modes opératoires, empêchant par là-même tout regroupement pertinent. Aussi est-il recommandé que soit mis en place un système d'assurance qualité et que soient placés sous scellés tous les prélèvements biologiques. Par ailleurs, ce fichier ne peut avoir de réelle efficacité que s'il s'étend sur l'ensemble de l'espace judiciaire européen. C'est pourquoi il lui demande quelles dispositions elle entend prendre pour remédier à l'inefficacité du fichier national d'empreintes génétiques dans sa forme actuelle et quelles démarches elle entend entreprendre auprès de nos partenaires de l'Union européenne afin de créer un véritable fichier national et européen d'empreintes génétiques.

Réponse : la garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que le fichier national automatisé des empreintes génétiques (FNAEG) est aujourd'hui entré dans une phase opérationnelle. La mise en oeuvre effective de ce fichier centralisé et informatisé de police judiciaire a nécessité des arbitrages à la fois techniques et juridiques. En effet, le recours à des méthodes scientifiques de prélèvement, d'analyse et de conservation de matériel biologique humain, implique que celles-ci offrent la fiabilité nécessaire à toute preuve scientifique dans le domaine de la justice pénale. C'est dans ce sens que se sont inscrites les actions de la chancellerie, sans négliger la perspective d'une extension du fichier ou d'échanges avec nos partenaires européens. L'effectivité de la loi du 17 juin 1998, qui a créé le FNAEG, a été assurée par plusieurs textes. Le décret n° 2000-413 du 18 mai 2000 a fixé les modalités d'enregistrement des données qui doivent figurer dans ce fichier et a organisé la conservation des prélèvements biologiques réalisés dans le cadre des articles 706-47 et suivants du code de procédure pénale. Dans son prolongement, une circulaire d'application a été adressée le 10 octobre 2000 aux procureurs généraux. Elle a été complétée par plusieurs dépêches en date des 26 mars, 23 mai et 18 juin 2001, donnant aux magistrats du parquet des instructions pour l'alimentation du fichier. L'attention des parquets généraux a été notamment appelée sur les prélèvements concernant les personnes définitivement condamnées. Des analyses sont actuellement en cours et viennent progressivement alimenter la base de données du fichier. De plus, les travaux d'un groupe de pilotage associant sous la présidence de la direction des affaires criminelles et des grâces, des représentants du ministère de l'Intérieur et du ministère de la Défense, ont permis de résoudre les difficultés techniques et juridiques soulevées par la mise en oeuvre du fichier. Il en est résulté la circulaire en date du 20 juillet 2001, qui a déterminé les modalités pratiques applicables à chaque stade de la procédure. Elle s'articule autour de deux principes : l'effectivité de l'alimentation du fichier et la fiabilité du circuit des scellés. Les méthodes de travail ont été unifiées à chaque étape de la procédure, notamment par l'utilisation d'un kit unique de prélèvement et par une traçabilité du circuit des scellés. Enfin, par arrêté en date au 7 avril 2001, M. Denys Millet, avocat général près la cour d'appel de Paris, a été nommé en qualité d'autorité de contrôle du fichier. Les trois autres membres composant la commission qui l'assiste ont été désignés, par arrêté du 15 juin dernier. L'ensemble de ces dispositions garantit la fiabilité et le contrôle des données enregistrées au fichier. Diverses mesures ont été prises pour permettre une montée en puissance du dispositif. La direction centrale de la police judiciaire, autorité gestionnaire du fichier, a procédé, tout comme la gendarmerie nationale en ce qui concerne la conservation des prélèvements biologiques, au recrutement et à l'affectation de personnels qualifiés. En outre, des locaux ont été

aménagés au sein de la sous-direction de la police scientifique et technique de la police nationale pour accueillir l'équipement informatique nécessaire au fonctionnement du fichier. Des travaux ont été effectués au sein des locaux de l'institut de recherches criminelles de la gendarmerie nationale, afin d'accueillir dans des conditions techniques optimales, les prélèvements placés sous scellé. Dans l'attente de l'installation définitive du service central de conservation des prélèvements biologiques dans de nouveaux locaux, les scellés peuvent, comme ils sont déjà actuellement, continuer à être stockés provisoirement au sein des greffes des juridictions. Depuis plusieurs mois, l'ensemble des acteurs judiciaires, ainsi que les services et unités d'enquête, ont été mobilisés. Tous sont aujourd'hui conscients de l'intérêt que ce nouveau mode de preuve scientifique présente pour la manifestation de la vérité, qu'il s'agisse de mettre hors de cause une personne soupçonnée ou de confondre un suspect. Ainsi, les parquets veillent à faire pratiquer dans les meilleurs délais les prélèvements sur les personnes définitivement condamnées pour les infractions à caractère sexuel. Les résultats des analyses seront adressés au FNAEG, aux fins d'inscription. Il y a lieu d'observer que les conditions de fonctionnement du fichier doivent également tenir compte des exigences de la coopération judiciaire entre les pays européens et plus largement entre tous les états participant à Interpol. Cette préoccupation a guidé la mise en place du système français. Le choix technique ont été opérés dans le but de permettre des échanges d'information, malgré une diversité des systèmes au sein de l'Union européenne. Néanmoins, les États retiennent des méthodes d'analyses standardisées afin de mettre en œuvre la résolution du 9 juin 1997 du conseil des ministres de l'Union européenne relative à l'échange des résultats des analyses d'ADN et les diverses recommandations des groupes de travail européens regroupant les membres d'Interpol. À terme, le FNAEG sera donc un instrument de coopération judiciaire internationale permettant de faire face au développement de la criminalité. C'est pourquoi, dès à présent, le fonctionnement du FNAEG est assuré, comme le Gouvernement s'y était engagé. En outre, l'analyse de l'ADN étant aujourd'hui un élément important de l'enquête, une extension du FNAEG est actuellement soumise à la représentation nationale dans le cadre du projet de loi « sécurité quotidienne ».

Sénat

Question n^2 : 34711 de M. **Turk Alex,** ministère interrogé : Intérieur
Réponse publiée au JO le : **22/11/2001** page 3715

Définition des « tendances » politiques des élus locaux

Question : M. Alex Turk attire l'attention de M. le ministre de l'Intérieur à propos des incohérences nombreuses relevées dans la définition des « tendances » politiques des élus locaux. En effet, nombre de maires se plaignent de se voir attribuer des étiquettes par les services du ministère sans avoir été en mesure de préciser eux-mêmes quelle pouvait être leur orientation politique. De même, ils s'interrogent sur les raisons pour lesquelles le ministère refuse de tenir compte du souhait de nombre d'entre eux d'être répertoriés sous l'appellation non-inscrit. Il lui demande quelles mesures il compte prendre pour dissiper ces ambiguïtés.

Réponse : l'attribution, par le ministère de l'Intérieur, d'une nuance politique aux candidats et aux élus lors des scrutins locaux et nationaux est ancienne. Le ministère assure en effet, depuis le début de la III^e République, la centralisation des résultats électoraux par appartenance politique. L'attribution d'une nuance politique est effectuée selon des critères parfaitement objectifs : la grille des nuances politiques, établie avant chaque scrutin, à un moment où les forces politiques en présence

sont stabilisées, énumère, pour faciliter l'analyse des résultats, les différentes appartenances au sein des familles politiques. La plupart du temps, la nuance attribuée au candidat n'est rien de plus que l'étiquette expressément choisie par celui-ci. Les seuls regroupements opérés concernent les élus qui, ne se réclamant d'aucun parti, se voient affecter une nuance plus générale, retenue à partir d'éléments objectifs tels que les déclarations publiques faites lors des campagnes électorales, les soutiens qu'il affiche à l'égard d'un parti ou les appuis dont il bénéficie de la part d'un parti. Pour procéder à ces classements, le ministère de l'intérieur disposait jusqu'à présent de fichiers d'élus ayant fait l'objet, en 1981, d'une déclaration à la commission nationale de l'informatique et des libertés, en application des dispositions de l'article 48 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le décret du 30 août 2001, pris sur avis conforme de la CNIL, autorise la création au ministère de l'intérieur d'un fichier nominatif unique des élus et des candidats aux élections au suffrage universel. Ce fichier permettra non seulement l'analyse politique des résultats des scrutins, la mise en ligne des résultats mais également, en permettant le croisement des données, le contrôle de l'application de la législation électorale relative, notamment, au cumul des mandats, à la parité, à l'interdiction des candidatures multiples. L'ensemble des informations contenues dans ce fichier sera totalement transparent puisque le décret prévoit de donner à chaque candidat ou candidat tête de liste pour les scrutins de liste, du moment du dépôt des candidatures, la grille des nuances politiques retenues pour le scrutin considéré. Les candidats seront en outre informés de la possibilité qui leur est ouverte d'avoir accès, à tout moment, au classement qui leur est affecté au sein de cette grille et de faire usage du droit de rectification prévu par l'article 36 de la loi du 6 janvier 1978. Par ailleurs, les données figurant dans ce fichier pourront être communiquées à toute personne sur simple demande et ne seront conservées que pendant la durée des mandats. Cet acte réglementaire est de nature à supprimer définitivement toutes les ambiguïtés soulignées par l'honorable parlementaire puisque, désormais, le classement par famille politique des candidats et des élus s'effectuera selon des modalités totalement transparentes, dans un souci d'information des citoyens et de respect des droits des personnes. S'agissant de l'attribution d'une nuance politique aux candidats et aux élus qui ne se réclament d'aucune appartenance, notamment lors des scrutins locaux qui sont en effet moins marqués par des enjeux de politique nationale, le décret précité a pris en compte cet état de fait et prévoit en conséquence qu'aucune information ne sera détenue sur les candidats aux élections municipales dans les communes de moins de 3 500 habitants. S'agissant des personnes élues dans cette strate de communes, seule sera enregistrée dans le fichier la nuance politique des maires. Cela signifie qu'aucune information sur l'appartenance politique des conseillers municipaux des communes de moins de 3 500 habitants ne figurera dans le fichier, même si ces élus seront néanmoins inclus dans le fichier pour l'application des autres finalités de celui-ci. L'ensemble du dispositif réglementaire répond parfaitement au souci exprimé par l'honorable parlementaire de ne pas attribuer unilatéralement une nuance politique lorsque les enjeux du scrutin, très locaux par définition, ne le justifient pas, tout en recensant néanmoins l'ensemble des élus afin d'informer le plus largement possible les citoyens sur les résultats des élections et de contrôler de la manière la plus efficace possible le respect de la législation électorale.

Annexe 8

La protection des données personnelles en Europe et dans le monde

1 — La protection des données dans l'Union européenne

Pays	Convention 108	Législation	Autorité de contrôle
Allemagne	Signature 28 janvier 1981 Ratification 18 juin 1985 En vigueur 1er octobre 1985	♦ Loi fédérale du 21 janvier 1977 portan protection contre l'emploi abusif de données d'iden ifica ion personnelle dans le cadre du traitement de données, modi iée par la loi fédérale de protection des données du 20 décembre 1990 (amendée par la loi du 14 septembre 1994) ♦ Transposition directive 95/46/CE : Federal Data Protec ion Act 2001. ♦ Législa ions des *Länder*	*Der Bundesbeauftragte für den Dalenschutz* (autori é édérale) Friedrich Ebert Strasse 1 53173 Bonn Allemagne Site web : www.datenschulz de
Autriche	Signature 28 janvier 1981 Ra ification 30 mars 1988 En vigueur 1er juillet 1988	♦ Loi édérale sur la protection des données du 18 octobre 1978 (amendée en 1986) ♦ Transposition directive 95/46/CE : Data protec ion act 2000	Direktor Buro der Datenschutzkommission und des Datenschutzraler Bundeskanzlerant Ballhausplatz 1 1014 Vienne site Web : www bka gv.at/datenschutz
Belgique	Signature 7 mai 1982 Ra ification 28 mai 1993 En vigueur 1er septembre 1993	♦ Loi relative à la protec ion de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992 ♦ Transposition directive 95/46/CE : loi du 11 décembre 1998 ♦ Arrêté royal du 13 mars 2001 portant exécu ion de la loi du 8 décembre 1992 rela ive à la protection des données personnelles	Commission de la protection de la vie privée Ministère de la Justice Boulevard de Waterloo 115 1000 Bruxelles Site web : www privacy.fgov.be
Danemark	Signature 28 janvier 1981 Ra ifica ion 23 octobre 1989 **En vigueur 1" février 1990**	♦ Loi n° 293 du 8 juin 1978 sur les registres privés et loi n' 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées en 1988 et en 1991 ♦ Transposition directive 95/46/CE : loi partielle du 1er octobre 1998 et loi n° 429 du 31 mai 2000	Datatilsynet Christians Brygge 28 4 sal 1559 Copenhague Site web : www data ilsynet.dk
Espagne	Signature 28 janvier 1982 Ra ifica ion 31 janvier 1984 En vigueur 1er octobre 1985	♦ Loi du 29 octobre 1992 réglementant le traitement automa isé de données personnelles ♦ Transposition directive 95/46/CE : loi du 13 décembre 1999	Agenda de Protec ion de Datos C/Sogasfa, **22** Madrid 28004 Site web : www.agenciaprotecciondatos es
Finlande	Signature 10 avril 1991 Ratifica ion 2 décembre 1991 **En vigueur 1er avril 1992**	♦ Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police ♦ Transposition directive 95/46/CE : loi n° 523 du 10 février 1999	Office of the Data Protection Ombusman **Albertinkatu 25** PO **Box 315** 00181 Helsinki Site web : www. ietosuoja.fi

France	Signature 28 janvier 1981 Ratifica ion 24 mars 1983 En vigueur l" octobre 1985	♦ Loi n° 78-17 du 6 janvier 1978 rela ive à l'informatique, aux fichiers et aux liber és ♦ Transposition direc ive 95/46/CE : projet de loi adopté en première lecture par l'Assemblée na ionale le 30 janvier 2002.	Commission na ionale de l'informa ique et des libertés 21, rue Saint-Guillaume 75340 Paris cedex 07 Site web : www.cnil.fr
Grèce	Signature 17 février 1983 Ratification 11 juin 1995 En vigueur 1er décembre 1995	♦ Loi n' 2472 sur la protec ion des personnes à l'égard du traitement des données à caractère personnel du 26 mars 1997 ♦ Transposition direc ive 95/46/CE : effectuée par la loi n° 2472 du 26 mars 1997	Commission pour la protec ion des données Omirou 8 PC 10564 A hènes Grèce Site web : www dpa.gr
Irlande	Signature 18 décembre 1986 Ra ifica ion 25 avril 1990 En vigueur!" août 1990	♦ Loi sur la protection des données du 13 juillet 1988 ♦ Transposi ion direc ive 95/46/CE : oi adop ée le 18 évrier 2002	Data protec ion commissioner Block 4, Irish Life Centre Talbot Street- Dublin 1 Irlande Site web : www dataprivacy ie
Italie	Signature 2 février 1983 Ratifica ion 29 mars 1997 En vigueur 1er juillet 1997	♦ Loi n° 675 du 31 décembre 1996 sur la protection des données personnelles, modifiée par plusieurs décrets législatifs de 1997,1998 et 1999 ♦ Loi n° 325 sur les mesures de sécurité dans le traitement des données personnelles du 3 novembre 2000	Garante per la protezione dei da i personali Piazza di Monte Citorion.121 00186 Rome Italie Site web : www garanteprivacy.it
Luxembourg	Signature 28 janvier 1981 Ratification 10 évrier 1988 En vigueur 1" juin 1988	♦ Loi du 31 mars 1979 réglementant 'utilisation des données nomina ives dans les traitements informa iques, (amendée en 1992) ♦ Transposi ion directive 95/46/CE : Projet de loi	Commission consulta ive à la protec ion des données 16, boulevard Royal 2934 Luxembourg
Pays-Bas	Signature 21 janvier 1988 Ratification 24 août 1993 En vigueur 1er décembre 1993	♦ Loi du 28 décembre 1988 sur la protection des données, complé ée par une loi du 21 juin 1990 sur les fichiers de police : ♦ Transposi ion directive 95/46/CE : loi du 6 juillet 2000	Data Protection Authority Prins Clauslaan 20 Pos bus 93374 -2509 AJ. S'Grovenhage Pays-Bas Site web : www.cbpweb.nl
Portugal	Signature 14 mai 1981 Ratifica ion 2 septembre 1993 En vigueur 1er janvier 1994	♦ Loi n° 10/91 du 29 avril 1991 sur la protection des données à caractère personnel face à l'informatique, amendée par une loi du 29 août 1994 ♦ Transposi ion directive 95/46/CE : loi n° 67/98 du 26 octobre 1998 sur la protec ion des données personnelles	Comissào Nacional de Potecçào de Dados Informa izados **148,** rue de Sao **Bento** 1200 Lisbonne Portugal Site web : www.cndp.pt
Royaume-Uni	Signature 14 mai 1981 Ratifica ion 26 août 1987 En vigueur!" décembre 1987	♦ Loi sur la protec ion des données du 12 juillet 1988. (Transposi ion direc ive 95/46/CE : loi du 16 juillet 1998 sur la protection des données. ♦ Loi sur l'accès à l'information du 30 novembre 2000	The office of informa ion Commissioner Wycliffe House - Water Lane Wilmslow — Cheshire SK9 5AF United Kingdom Site web : www dataprotection gov.uk

Suède	Signature 28 janvier 1981 Ratifica ion 29 septembre 1982 En vigueur 1er octobre 1985	♦ Loi du 11 mai 1973 sur la protec ion des données ♦ Transposition direc ive 95/46/Œ : loi n° 204 du 24 octobre 1998 sur la protection des données	Datainspektionen Box 8114 104 20 Stockholm Suède Site web : www datainspek ionen se

2 — La protection des données dans le monde

Pays	Convention 108	Législation	Autorités de contrôle/contacts
Albanie		♦ Loi n° 8517 sur la protection des données personnelles 1999	
Afrique du Sud		♦ Promotion of access to informa ion act 2000	
Argentine		♦ Loi n° 25 326 sur la protection des données personnelles 2 novembre 2000	Direccion nacional de Dotos Personales Sarmiento 329 — Piso 5° 1041 Buenos Aires Argen ina
Australie		♦ Loi fédérale sur la vie privée 1988 (secteur public), amendement visant à étendre la protection des données dans e secteur privé 6 décembre 2000	Federal Privacy Commission GPO Box 5218 - Sydney NSW 1024 Site web : www privacy.gov au
Bulgarie	Signature 2 juin 1998	♦ Projet de loi en préparation	
Canada		♦ Loi fédérale sur la protection des renseignements personnels 1982 ♦ Loi fédérale sur la protection des renseignements personnels et les documents électroniques 2000	Federal privacy commission Tower B, 3rd Floor, 112 Kent Street - Otawa, Ontario K1A 1H3 Canada Site web : www privcom.gc.ca
Chypre	Signature 27 juillet 1986	♦ Loi adoptée en novembre 2001	
Corée du sud		♦ Loi sur la protec ion des données personnelles 1994	
Estonie	Signature 24 janvier 2000	♦ Loi sur la protec ion des données personnelles 1997	Estonien Data Protec ion Inspektorate Pikk 61 15 065 Tallinn Estonia Site web : www dp gov ee
États-Unis		♦ Loi sur la protec ion des libertés ndividuelles dans les administra ions fédérales 1974 ♦ Diverses lois sectorielles relatives à la protection des données Ex : he Fair Credit Repor ing Act (FCRA) 1970 (1) : The video privacy protection Act-1988 : Electronic Freedom of Information Act - 1996 : Children's Online Privacy Protection Act - 1998 (1)	(1) : Federal Trade Commission FTC 600 Pennsylvania Avenue NW DC 25080 Washington USA

Pays	Convention 108	Législation	Autorités de contrôle/contacts
Guernsey	Par extension En vigueur 1" décembre 1987	♦ Loi sur la protec ion des données 1986 ♦ Projet de loi modificatif 26 juillet 2000	The data protection officer PO Box 43 La Charroterie St Peter Port Guernesey G71 IFH Site web : www.dpcommission.gov.gg
Hong Kong		♦ Lai sur la protec ion des données 1990 ♦ Ordonnance sur la protec ion des données 1995	Privacy commission for Personal data Unit 2001, 20/F - OfficeTower Conven ion Plaza -1 Harbour Road Wan Chai — Hong Kong Site web : www.pco.org hk
Hongrie	Signature 13 mai 1993 Ratification 8 octobre 1997 En vigueur 1" évrier 1998	♦ Loi sur la protection des données personnelles et la communication de données publiques 1992	Parliamentary commissioner for data protection and freedom of information Tüköry **u** 3 H-1054 Budapes Hongrie Site web : www.obh.hu
Île de man	Par extension En vigueur 21 janvier 1993	♦ Loi sur la protection des données 1986	Data protec ion registrar PO Box 69 Douglas **M99 1EQ** — **île** de **Mon**
Inde		♦ The information technology act 9 juin 2000	
Islande	Signature 27 septembre 1982 Ra ifica ion 25 mars 1991 En vigueur 1° juillet 1991	♦ Loi n° 63-1981 relative 'enregistrement de données personnelles 1981 (amendée en 1989) ♦ Incorporation dans le droit national de a directive **95/46/CE** : loi n° 77 du 23 mai 2000 au titre de l'accord économique européen	Personuvernd Rauâararstig 10 105 Reykjavik Iceland Site web : www.personuvernd is
Israël		♦ Loi n' 5741 sur la protection de la vie privée 1981 (amendée en 1985 et 1996) ♦ Loi n° 5746 sur la protection des données dans l'administra ion 1986	Registrar of data bases Hashlodia 2 Yad Eliahu POB Israël 9288 Tel Aviv
Japon		♦ Loi sur la protec ion des données personnelles informa isées dans le secteur public 1988 ♦ Projet de loi dans le secteur privé mai 2001	Personnal Data Protection Task Force 1-6-1 Nagata Cho Chiyoda-ku 1008914 Tokyo Japon
Jersey	Par extension En vigueur 1" décembre 1987	♦ Loi sur la protection des données 1987	Data protection registry Marier House Halckett Place Saint Helier Jersey JE1 1DD
Lettonie	Signature 31 octobre 2000	♦ Loi sur la protec ion des données avril 2000	Ministry of Justice Departement of European Affairs Brivibas boulevard 36 Riga, LV 1050 Latvia

Pays	Convention 108	Législation	Autorités de contrôle/contacts
Lituanie	Signature 11 février 2000	♦ Loi sur la protec ion des données personnelles 1996 (amendée en 2000)	State Data Protec ion Inspectorate Gedimino ave 27/2 LT -2600 Vilnius Li huania Site web : www is.lt/dsinsp
Moldavie	Signature 4 mai 1998		
Monaco		♦ Loi n° 1165 relative aux traitements d'informations nomina ives 1993	Commission de contrôle des informa ions nomina ives Gildor Pastor Center, 7, rue du Gablan Bloc B — Bureau 409 98000 Monaco
Norvège	Signature 13 mars 1981 Ra ifica ion 20 février 1984 **En vigueur 1er octobre 1985**	♦ Loi sur les registres de données personnelles 1978 ♦ Incorporation dans le droit national de a directive 95/46/CE : loi du 14 avril 2000 au itre de l'accord économique européen.	Datatilsynet Postboks 8177 Dep 0034 Oslo 1 Norvège Site web : www data ilsynet no
Nouvelle-Zél ande		♦ Loi sur l'information du secteur public 17 décembre 1982 ♦ Loi sur la vie privée 1993	Privacy commission PO Box 466 Auckland Nouvelle-Zélande Site web : www.privacy.org nz
Paraguay		♦ Loi sur la protec ion des données 28 décembre 2000	
Pologne	Signature 21 avril 1999	♦ Loi sur la protec ion des données personnelles 1997	Biuro Geneeralnego Inspektora PowstancowWarszawyl PL 00-030 Warszawa Pologne Site web: www.giodo gov.pl
République de Saint-Marin		♦ Loi rela ive à la protec ion des données personnelles 1983 (amendée en 1995)	
République Tchèque	Signature 8 septembre 2000 Rati iée 9 juillet 2001	♦ Loi relative à la protection des données personnelles des systèmes nformatisés 1992 ♦ Loi n° 101/2000 sur la protection des données personnelles 1er juin 2000	Office for Personal Data Protection Havelkova 22, CZ-13000 Praha 3 Czech Republic Site web : www uoou.cz
République de Macédoine		♦ Loi sur la protection des données personnelles 1994	
Roumanie	Signature 18 mars 1997	♦ Loi rela ive à la protection des données à carac ère personnel : n° 677/2001 JO n° 790 **du** 12 décembre 2001	Le Médiateur des Droits de l'Homme B-dul lancu de Hunedoara nr. 3-5 Sector 1 Bucures i Romania
Russie		♦ Loi édérale sur l'information, 'informatisation et la protection ' des informa ions 1995	

Pays	Convention 108	Législation	Autorités de contrôle/contacts
Slovaquie	Signature 14 avril 2000 Ratification 13 septembre 2000 En vigueur 1er janvier 2001	♦ Loi relative à la protection des données personnelles des systèmes informatisés 1998	Office for the Protection of Personal Data Urad Vlady SR Namestie Slobody 1 813 70 Bratislava I Slovak Republic
Slovénie	Signature 23 novembre 1993 Ratification 27 mai 1994 En vigueur 1er septembre 1994	♦ Loi n° 210-01/89-3 sur la protection des données 1999	Namestnik varuha clovekovih pravic Urad varuha clovekovih pravic Dunajska 56 SI-1000 Ljubljana Slovénie
Suisse	Signature 2 octobre 1997 Ratification 2 octobre 1997 En vigueur 1er février 1998	♦ Loi fédérale sur la protection des données 1992	Commissaire à la protection des données Feldeggweg 1 CH-3003 Berne SUISSE Site web : www.edsb.ch
Taiwan		♦ Loi sur la protection des données 1995	The ministry of justice 130, Sec 1, Chung Ching South Road Taipei 100 —Taiwan
Thaïlande		♦ Loi sur la protection des données dans le secteur public 1998	Authority for the protection of Personal Data Information Commission Government House Bangkok 10300 Thailand
Turquie	Signature 28 janvier 1981	♦ Projet de loi	

3 — Communautés européennes et organisations internationales

Communauté européenne	Directive européenne n° 95/46/CE relative à a protection des personnes physiques à égard des données à caractère personnel et à a libre circulation de ces données 24 octobre 1995	Commission européenne DG marché intérieur 200 rue de la Loi-Bruxelles B-1049 Belgique Site web : http://europa.eu.int/comm/internal market/fr/index.htm
Conseil de l'Europe	Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 28 janvier **1981**	Conseil de l'Europe Direction des affaires juridiques Section protection des données Avenue de l'Europe 67075 Strasbourg — France Site web : www.legal.coe.int/dataprotection
OCDE	Lignes directrices régissant la protection de a vie privée et les flux transfrontières de données à caractère personnel 23 septembre **1980**	OCDE 2, rue André Pascal 75775 Paris cedex 16 Site web : www.oecd.org/index-fr.htm
ONU	Lignes directives pour la réglementation des fichiers informatisés de données à caractère personnel 1989	Site web : www.unhchr/french/html/inllinst fr.htm

Annexe 9

Décisions de la Commission européenne

DÉCISION DE LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES DU 15 JUIN 2001 RELATIVE AUX CLAUSES CONTRACTUELLES TYPES POUR LE TRANSFERT DE DONNÉES À cARACTÈRE PERSONNEL VERS DES PAYS TIERS EN VERTU DE LA DIRECTIVE 95/46/CE[1]
[notifiée sous le numéro C (2001) 1539]

(Texte présentant de l'intérêt pour l'EEE)

La Commission des communautés européennes ;

vu le traité instituant la Communauté européenne ;

vu la directive *95/46/CE* du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2], et notamment son article 26, paragraphe 4 ;

considérant ce qui suit :

Conformément à la directive 95/46/CE, les États membres sont tenus de veiller à ce qu'un transfert de données à caractère personnel vers un pays tiers ne puisse avoir lieu que si le pays en question assure un niveau de protection adéquat des données et si les lois des États membres, qui sont conformes aux autres dispositions de la directive, sont respectées avant le transfert.

Toutefois, l'article 26, paragraphe 2, de la directive 95/46/CE prévoit que les États membres peuvent autoriser, sous certaines garanties, un transfert, ou un ensemble de transferts, de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat. Ces garanties doivent notamment résulter de clauses contractuelles appropriées.

Conformément à la directive 95/46/CE, le niveau de protection des données doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel instauré au titre de ladite directive[3], a publié des lignes directrices afin de faciliter l'évaluation[4].

---

1 JO L181 du 4 juillet 2001, p. 19.
2 3 *JO L* 281 du 23 novembre 1995, p. 31.
L'adresse Internet du groupe de travail est la suivante :
http://www.europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs/index.htm
4 1 WP 4 (5020/97) « Premières orientations relatives aux transferts de données personnelles vers des pays
tiers — Méthodes possibles d'évaluation du caractère adéquat de la protection », document de réflexion adopté par le groupe de travail le 26 juin 1997 ;
WP 7 55057/97) « Évaluation des codes d'autoréglernentation sectoriels : quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers ? », document de travail adopté par le groupe de travail le 14 janvier 1998 ;
WP 9 (5005/98) « Vues préliminaires sur le recours à des dispositions contractuelles dans le cadre de transferts de données à caractère personnel vers des pays tiers », document de travail adopté par le groupe de travail le 22 avril 1998 ;
WP 12 : « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données », document adopté par le groupe de travail le 24.7 1998 et disponible sur le site Web « europa. eu. int/comm/internal_markt/fr/media.dataprot/wpdocs/ » de la Commission européenne.

L'article 26, paragraphe 2, de la directive 95/46/CE, qui assure la flexibilité à une organisation qui souhaite transférer des données vers des pays tiers, et l'article 26, paragraphe 4, qui prévoit des clauses contractuelles types, sont essentiels pour assurer le flux nécessaire de données à caractère personnel entre la Communauté et les pays tiers sans imposer de charges inutiles aux opérateurs économiques. Lesdits articles sont particulièrement importants étant donné que la Commission n'adoptera probablement des mécanismes attestant le niveau adéquat de protection des données, conformément à l'article 25, paragraphe 6, que pour un nombre limité de pays à court terme ou même à moyen terme.

Les clauses contractuelles types ne constituent qu'une des diverses possibilités prévues par la directive *95/46/CE,* pour transférer de manière licite des données à caractère personnel conjointement aux articles 25 et 26, paragraphes 1 et 2. En intégrant ces clauses contractuelles dans un contrat, les organisations pourront transférer beaucoup plus aisément des données à caractère personnel vers des pays tiers. Les clauses contractuelles types ne concernent que la protection des données et l'exportateur de données et l'importateur de données sont libres d'inclure d'autres clauses à caractère commercial, comme des clauses d'assistance mutuelle en cas de litiges avec une personne concernée ou une autorité de contrôle, qu'ils jugent pertinentes pour le contrat à condition qu'elles ne contredisent pas les clauses contractuelles types.

La présente décision ne doit pas affecter les autorisations nationales que les États membres peuvent délivrer conformément aux dispositions nationales mettant en œuvre l'article 26, paragraphe 2, de la directive *95/46/CE.* Les circonstances des transferts spécifiques peuvent amener les responsables du traitement des données à prévoir des garanties différentes au sens de l'article 26, paragraphe 2. En tout état de cause, la présente décision a pour seul effet d'obliger les États membres à ne pas refuser de reconnaître que les clauses contractuelles qui y sont décrites offrent des garanties adéquates et elle n'a donc aucun effet sur d'autres clauses contractuelles.

Le champ d'application de la présente décision se limite à établir que les clauses reprises dans l'annexe peuvent être utilisées par un responsable du traitement établi dans la Communauté pour offrir des garanties suffisantes au sens de l'article 26, paragraphe 2, de la directive *95/46/CE.* Le transfert de, données à caractère personnel vers des pays tiers constitue un traitement dans un État membre dont la licéité est soumise au droit national. Dans l'exercice des fonctions et des pouvoirs qui leur sont conférés par l'article 28 de la directive *95/46/CE,* les autorités de contrôle des États membres demeureront compétentes pour apprécier si l'exportateur de données a respecté le droit national mettant en œuvre les dispositions de la directive *95/46/CE* et, notamment, toute règle spécifique relative à l'obligation de fournir des informations au titre de la directive.

La présente décision ne couvre pas le transfert de données à caractère personnel effectué par des responsables du traitement établis dans la Communauté vers des destinataires établis en dehors du territoire de la Communauté qui agissent exclusivement en tant que sous-traitants. Ces transferts n'exigent pas les mêmes garanties parce que le sous-traitant agit exclusivement pour le compte du responsable du traitement. La Commission estime qu'il est nécessaire d'aborder ce transfert dans une décision ultérieure.

Il convient d'établir les informations minimales que les parties doivent prévoir dans le contrat qui a trait au transfert. Les Etats membres doivent conserver la faculté de spécifier les informations que les parties doivent fournir. L'application de la présente décision sera revue à la lumière de l'expérience acquise.

La Commission examinera à l'avenir également si les clauses contractuelles types présentées par des organisations commerciales ou d'autres parties concernées offrent des garanties suffisantes conformément à l'article 26, paragraphe 2, de la directive 95/46/CE.

Tandis que les parties doivent être libres de convenir des règles de protection des données de fond que l'importateur de données doit respecter, certains principes de protection des données doivent s'appliquer en tout état de cause.

Les données ne doivent être traitées et ensuite utilisées ou être communiquées à d'autres qu'à des fins déterminées et ne doivent pas être conservées plus longtemps que nécessaire.

Conformément à l'article 12 de la directive 95/46/CE la personne concernée doit avoir un droit d'accès à toutes les données la concernant et le cas échéant un droit de rectification, d'effacement ou d'opposition à certaines données.

D'autres transferts de données à caractère personnel à un autre responsable du traitement établi dans un pays tiers ne doivent être permis que sous certaines conditions, visant en particulier à garantir que les personnes concernées reçoivent des informations correctes et ont la possibilité de s'opposer, ou dans certains cas de retirer leur consentement.

Outre l'appréciation de la conformité des transferts vers des pays tiers avec le droit national, les autorités de contrôle doivent également jouer un rôle-clé dans ce mécanisme contractuel en garantissant la protection adéquate des données à caractère personnel après le transfert. Dans les circonstances particulières, les autorités de contrôle des États membres doivent conserver la faculté d'interdire ou de suspendre un transfert de données ou un ensemble de transferts basé sur des clauses contractuelles types dans les cas exceptionnels où il est établi qu'un transfert basé sur des termes contractuels risque d'altérer considérablement les garanties offrant un niveau de protection adéquat à la personne concernée.

Les clauses contractuelles types doivent être exécutoires, non seulement par les organisations parties au contrat mais également par les personnes concernées, en particulier lorsque ces dernières subissent un dommage en raison d'une rupture du contrat.

Le droit régissant le contrat doit être le droit de l'État membre dans lequel l'exportateur de données est établi qui autorise un tiers bénéficiaire à faire exécuter un contrat. Les personnes concernées doivent pouvoir être représentées par des associations ou d'autres organismes si elles le souhaitent et si le droit national l'autorise.

Pour réduire les difficultés d'ordre pratique que les personnes concernées pourraient rencontrer lorsqu'elles tentent de faire appliquer leurs droits en vertu de ces clauses contractuelles types, l'exportateur de données et l'importateur de données doivent être solidairement responsables des dommages résultant de toute violation des dispositions soumises à la clause du tiers bénéficiaire.

La personne concernée a le droit d'exercer un recours et d'obtenir réparation de l'exportateur de données, de l'importateur de données ou des deux pour tout dommage résultant de toute action incompatible avec les obligations prévues par les clauses contractuelles types. Les deux parties peuvent être exonérées de cette responsabilité si elles prouvent que ni l'une ni l'autre n'étaient responsables.

La responsabilité solidaire ne s'étend pas aux dispositions non couvertes par la clause du tiers bénéficiaire et elle ne doit pas rendre une partie responsable du traitement illicite effectué par l'autre partie. Bien qu'un dédommagement mutuel entre les parties ne soit pas obligatoire pour garantir le niveau adéquat de protection des personnes concernées et que cette disposition puisse donc être supprimée, elle

est incluse dans les clauses contractuelles types dans un souci de clarification et pour éviter aux parties de devoir négocier des clauses de dédommagement séparément.

Si un litige entre les parties et la personne concernée n'est pas résolu à l'amiable et si la personne concernée invoque la clause du tiers bénéficiaire, les parties conviennent de proposer à la personne concernée le choix entre la médiation, l'arbitrage ou le procès. La médiation par l'autorité de contrôle d'un État membre doit être une option lorsqu'elle fournit un tel service.

Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué en vertu de l'article 29 de la directive 95/46/CE a émis un avis sur le niveau de protection prévu par les clauses contractuelles types annexées à la présente décision, cet avis a été pris en considération dans la préparation de la décision actuelle[1].

Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué en vertu de l'article 31 de la directive 95/46/CE ;

A ARRÈTÉ LA PRÉSENTE DÉCISION :

Article premier

Les clauses contractuelles types contenues dans l'annexe sont considérées comme offrant des garanties suffisantes en matière de protection de la vie privée et des droits fondamentaux et libertés des individus et en ce qui concerne l'exercice des droits correspondants comme l'exige l'article 26, paragraphe 2, de la directive 95/46/CE.

Article 2

La présente décision concerne uniquement le caractère adéquat de la protection fournie par les clauses contractuelles types pour le transfert de données à caractère personnel contenues en annexe. Elle n'affecte pas l'application d'autres dispositions nationales mettant en oeuvre la directive *95/46/CE* qui se rapportent au traitement de données à caractère personnel dans les États membres.

La présente décision ne s'applique pas au transfert de données à caractère personnel par des responsables du traitement établis dans la Communauté à des destinataires établis en dehors de la Communauté qui agissent seulement comme sous-traitants.

Article 3

Aux fins de la présente décision :
(a) les définitions contenues dans la directive 95/46/CE s'appliquent ;
(b) les « catégories spéciales de données » sont les données visées à l'article 8 de la dite directive ;
(c) les « autorités de contrôle » sont les autorités visées à l'article 28 de ladite direc tive ;
(d) l'« exportateur de données » est le responsable du traitement qui transfère les données à caractère personnel ;
(e) l'« importateur de données » est le responsable du traitement qui accepte de rece voir de l'exportateur de données des données de caractère personnel en vue de leur traitement ultérieur conformément aux conditions de la présente décision.

[1] Avis n° 1 /2001 adopté par le groupe de travail le 26 janvier 2001 (DG MARKT 5102/00/WP 38), disponible sur le site web « Europa » de la Commission européenne.

Article 4

1 — Sans préjudice de leurs pouvoirs de prendre des mesures visant à assu rer le respect des dispositions nationales adoptées conformément aux chapitres II, III, V et VI de la directive 95/46/CE, les autorités compétentes des États membres peu vent exercer les pouvoirs dont elles disposent pour interdire ou suspendre les flux de données vers des pays tiers afin de protéger les individus en ce qui concerne le traite ment de leurs données à caractère personnel, et ce dans les cas où :
(a) il est établi que le droit auquel l'importateur de données est soumis oblige ce der nier à déroger aux règles pertinentes de protection des données au-delà des restric tions nécessaires dans une société démocratique comme le prévoit l'article 13 de la directive 95/46/CE lorsque ces obligations risquent d'altérer considérablement les garanties offertes par les clauses contractuelles types, ou ;
(b) une autorité compétente a établi que l'importateur de données n'a pas respecté les clauses du contrat ou ;
(c) il est fort probable que les clauses contractuelles types en annexe ne sont pas ou ne seront pas respectées et que la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves.

2 — L'interdiction ou la suspension conformément au paragraphe 1 est levée dès que les raisons qui la motivaient disparaissent.

3 — Lorsque les États membres adoptent des mesures conformément aux pa ragraphes 1 et 2, ils informent sans délai la Commission, qui transmet l'information aux autres États membres.

Article 5

La Commission évalue l'application de la présente décision, sur la base des informations disponibles, trois ans après sa notification aux États membres. Elle com-munique au comité institué au titre de l'article 31 de la directive 95/46/CE un rapport sur les constatations effectuées. Le rapport comprend tout élément susceptible d'influer sur l'évaluation concernant l'adéquation des clauses contractuelles types figurant en annexe et tout élément indiquant que la présente décision est appliquée de manière discriminatoire.

Article 6

La présente décision s'applique à compter du 3 septembre 2001.

Article 7

Les États membres sont destinataires de la présente décision.

ANNEXE
Clauses contractuelles types

aux fins de l'article 26, paragraphe 2, de la directive 95/46/CE pour le transfert de données à caractère personnel vers des pays tiers qui n'assurent pas un niveau adéquat de protection

Nom *de l'organisation exportant des données :* .....
Adresse : .....

Tél. **:** .....***Fax*** **:** .....***Courrier électronique*** **:** .....
Autres informations nécessaires pour identifier l'organisation : .....
(ci-après dénommé « **l'exportateur** de données »)

d'une part, et

Nom de *l'organisation* : .....
Adresse : .....
Tél.* : ..... Fox : ..... *Courrier électronique : .....
***Autres informations nécessaires pour identifier l'organisation* : .....**
(ci-après dénommé « **l'importateur** de données »)

d'autre part,

Sont convenus des clauses contractuelles suivantes (ci-après dénommées « les **clauses** ») afin d'offrir des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes lors du transfert, par l'exportateur de données vers l'importateur de données, des données à caractère personnel visées dans l'appendice 1.

Clause première
Définitions

Au sens des clauses :
(a) « *données à caractère personnel* », « *catégories spéciales de données* », « *traiter/traitement* », « *responsable du traitement* », « *sous-traitant* », « *personne concernée* » et « *autorité de contrôle* » ont la même signification que dans la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommée « la **directive ») ;**
b) « l'*exportateur de données* », est le responsable du traitement qui transfère les données à caractère personnel ;
(c) « *l'**importateur de données*** », est le responsable du traitement qui accepte de recevoir les données à caractère personnel de l'exportateur de données pour les traiter ultérieurement conformément aux présentes clauses et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate.

Clause 2
Détails du transfert

Les détails du transfert, et en particulier les catégories de données à caractère personnel et les finalités pour lesquelles elles sont transférées, sont spécifiés dans l'appendice 1 qui fait partie intégrante des présentes clauses.

Clause 3
Clause du tiers bénéficiaire

1 Les personnes concernées peuvent faire appliquer la présente clause ainsi que la clause 4 (b), (c) et (d), la clause 5 (a), (b), (c), (e), 6 (1), (2), les clauses 7, 9 et 11 en tant que tiers bénéficiaires. Les parties ne s'opposent pas à ce que les personnes concernées soient représentées par une association ou d'autres organismes si elles le souhaitent et si le droit national le permet.

Clause 4
Obligations* de *l'exportateur de données

L'exportateur de données accepte et garantit ce qui suit :
a) le traitement des données à caractère personnel effectué par ses soins, y compris e transfert proprement dit, a été et continuera d'être, jusqu'au moment du transfert, effectué conformément à l'ensemble des dispositions pertinentes de l'État membre où l'exportateur des données est établi (et, le cas échéant a été notifié aux autorités compétentes) et ne viole pas les dispositions pertinentes dudit État ;

(b) si le transfert porte sur des catégories spéciales de données, les personnes concer nées ont été informées ou seront informées avant le transfert que leurs données pour raient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat ;
(c) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des présentes clauses telles que convenues et ;
(d) il répondra, dans des délais raisonnables et dans la mesure du possible, aux de mandes de renseignements de l'autorité de contrôle relatives au traitement des don nées pertinentes à caractère personnel effectué par l'importateur et à toute demande de la personne concernée quant au traitement de ses données à caractère personnel par l'importateur..

Clause 5

Obligations de l'importateur de données

L'importateur de données accepte et garantit ce qui suit :
(a) il n'a aucune raison de croire que la législation le concernant l'empêche de rem plir ses obligations prévues par le contrat, et qui en cas de modification de cette légis lation susceptible d'avoir des conséquences négatives importantes sur les garanties offertes par les clauses, il communiquera le changement à l'exportateur de données et à l'autorité de contrôle où l'exportateur de données est établi, auquel cas, l'expor tateur de données a le droit de suspendre le transfert des données et/ou de résilier le contrat ;
(b) il traitera les données à caractère personnel conformément à l'ensemble des prin cipes obligatoires de protection des données figurant dans l'appendice 2 ;
ou, sous réserve de l'accord exprès des parties, exprimé en cochant ci-dessous, et sous réserve du respect des « principes obligatoires de protection des données » fi-gurant dans l'appendice 3, il traitera à tous autres égards les données conformé-ment :
— aux dispositions pertinentes du droit national liés à ces clauses protégeant les li bertés et droits fondamentaux des personnes physiques, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans le pays où l'exportateur de données est établi, ou ;
— aux dispositions pertinentes prévues de toute décision de la Commission prise conformément à l'article 25, paragraphe 6 de la directive 95/46/CE constatant qu'un pays tiers assure un niveau de protection adéquat dans certains secteurs d'acti vité uniquement, à condition que l'importateur de données soit établi dans ce pays tiers et ne soit pas soumis à ces dispositions, pour autant que lesdites dispositions soient de nature à pouvoir être appliquées au secteur du transfert.
(c) il traitera de manière appropriée et en temps opportun toutes les demandes de renseignements raisonnables émanant de l'exportateur de données ou des personnes concernées et relatives au traitement effectué par ses soins des données à caractère personnel qui font l'objet du transfert et il coopérera avec l'autorité de contrôle com pétente lors de toutes les demandes de renseignements de cette dernière et se range ra à l'avis de cette même autorité en ce qui concerne le traitement des données transférées ;
(d) à la demande de l'exportateur de données, il soumettra ses moyens de traitement de données à une vérification qui sera effectuée par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, choisi par l'exportateur de données et le cas échéant avec raccord de l'autorité de contrôle ;
(e)il mettra à la disposition des personnes concernées, si elles le demandent, une copie des présentes clauses telles que convenues, et il signalera le bureau qui traite les plaintes.

Clause 6
Responsabilité

2 — Les parties conviennent que les personnes concernées ayant subi un dommage du fait d'une violation des dispositions visées à la clause 3 ont le droit d'obtenir des parties réparation du préjudice subi. Les parties conviennent qu'elles ne peuvent être exonérées de cette responsabilité que si elles prouvent que l'action incompatible avec les obligations prévues par les présentes clauses n'est imputable à aucune d'entre elles.

3 — L'exportateur de données et l'importateur de données conviennent d'être solidairement responsables des dommages subis par les personnes concer nées résultant d'une violation visée au paragraphe 1. En cas d'une telle violation, la personne concernée peut poursuivre en justice l'exportateur de données, l'importa teur de données ou les deux à la fois.

4 — Les parties conviennent que si l'une d'entre elles est tenue responsable d'une violation visée au paragraphe 1 commise par l'autre partie, la seconde partie dédommagera, dans la mesure où elle est responsable, la première partie de tout coût, charge, dommage, dépense ou perte encourue par la première partie (le para graphe 3 est optionnel).

Clause 7
Médiation et juridiction

1 — Les parties conviennent que dans le cas d'un litige entre une personne concernée et l'une ou l'autre des parties qui n'est pas résolu à l'amiable et pour le quel la personne concernée invoque la disposition du tiers bénéficiaire visée à la clause 3, elles acceptent la décision de la personne concernée :
(a) de soumettre le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle ;
(b) de porter le litige devant les tribunaux de l'État membre où l'exportateur de don nées est établi ;

2 — Les parties conviennent que d'un commun accord entre une personne concernée et la partie en question, un litige peut être porté devant un organe d'arbi trage si cette partie est établie dans un pays qui a ratifié la convention de New York sur la reconnaissance et l'exécution des sentences arbitrales.

3 — Les parties conviennent que les paragraphes 1 et 2 s'appliquent sans préjudice du droit procédural ou matériel de la personne concernée d'obtenir répa ration conformément à d'autres dispositions du droit national ou international.

Clause 8
Coopération avec les autorités de contrôle

Les parties conviennent de déposer une copie du présent contrat auprès de l'autorité de contrôle si un tel dépôt est prévu par le droit national.

Clause 9
Résiliation des clauses

Les parties conviennent que la résiliation des présentes clauses à quelque moment, dans quelque circonstance et pour quelque raison que ce soit ne les exonère pas des obligations et/ou conditions prévues par les présentes clauses à l'égard du traitement des données transférées.

Clause 10

Droit applicable

Les clauses sont régies par le droit de l'Etat membre dans lequel l'exportateur de données est établi à savoir.....

Clause 11

Modification du contrat

Les parties s'engagent à ne pas modifier les termes des présentes clauses.

Au nom de l'exportateur de données ;

Nom (écrit en toutes lettres) :.....
Fonction : .....
Adresse : .....
Autres informations nécessaires pour que le contrat soit un acte contraignant (le cas échéant) : .....
Signature :.....
(sceau de l'organisation)

Au nom de l'importateur de données ;

Nom (écrit en toutes lettres) :.....
Fonction : .....
Adresse : .....
Autres informations nécessaires pour valider le contrat en tant qu'acte contraignant (le cas échéant) :.....
Signature :.....
(sceau de l'organisation)

Appendice 1

Le présent appendice fait partie des clauses et doit être complété et signé par les parties

(* Les États membres peuvent apporter ou préciser, selon leurs procédures nationales, toute information supplémentaire nécessaire qui doit être contenue dans le présent appendice)

Exportateur de données

L'exportateur de données est *(veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert)* :

……
……

Importateur de données

L'importateur de données est *(veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert)* :

……
……

Personnes concernées

Les données à caractère personnel transférées concernent les catégories suivantes de personnes concernées *(veuillez préciser)* ;

……
……

Finalités du transfert

Le transfert est nécessaire pour les finalités suivantes *(veuillez préciser)* :

……
……

Catégories de données

Les données à caractère personnel transférées concernent les catégories suivantes de données *(veuillez préciser) :*

……
……

Données sensibles (le cas échéant)

Les données à caractère personnel transférées concernent les catégories suivantes de données sensibles *(veuillez préciser)* :

……
……

Destinataires

Les données à caractère personnel transférées ne peuvent être divulguées qu'auprès des destinataires suivants ou des catégories suivantes de destinataires *(veuillez préciser) :*

……
……

Limite de conservation

Les données à caractère personnel transférées ne peuvent pas être conservées plus de *(veuillez indiquer la durée) : .....* (mois/années)

EXPORTATEUR DE DONNÉES IMPORTATEUR DE DONNÉES

Nom :..... .....

Signature autorisée : .....

APPENDICE 2 aux clauses contractuelles types

Principes obligatoires de protection des données visés au paragraphe 1 de la clause 5 (b)

Les présents principes doivent être lus et interprétés à la lumière des dispositions (principes et exceptions pertinentes) de la directive 95/46/CE[1].

Ils s'appliquent sous réserve des exigences impératives de la législation nationale applicables à l'importateur de données qui ne vont pas au delà de ce qui est nécessaire dans une société démocratique sur la base de l'un des intérêts énumérés à l'article 13, paragraphe 1, de la directive *95/46/CE,* c'est-à-dire, si elles constituent une mesure nécessaire pour sauvegarder la sécurité de l'État, la défense, la sécurité

[1] Directive *95/46/CE* du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Journal officiel des Communautés européennes,* L 281 du 23 novembre 1995, p. 31.

publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées, un intérêt économique ou financier d'un Etat ou la protection de la personne concernée ou des droits et libertés d'autrui.

1) **Limitation des transferts à une finalité spécifique**

Les données ne doivent être traitées et utilisées ou communiquées ultérieurement que pour les finalités spécifiques indiquées dans l'appendice 1 aux présentes clauses. Elles ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles sont transférées.

2) **Qualité et proportionnalité des données**

Les données doivent être exactes et, au besoin, actualisées. Elles doivent être adéquates, pertinentes et non excessives au regard des finalités auxquelles obéit leur transfert ou leur traitement ultérieur.

3) **Transparence**

Les personnes concernées doivent recevoir des informations sur les finalités du traitement et sur l'identité du responsable de ce traitement dans le pays tiers ainsi que d'autres informations, dans la mesure où elles sont nécessaires pour assurer un traitement loyal, à moins que ces informations aient déjà été fournies par l'exportateur de données.

4) **Sécurité et confidentialité**

Le responsable du traitement doit prendre des mesures de sécurité, sur le plan technique et au niveau de l'organisation, qui soient appropriées au regard des risques présentés par le traitement, comme l'accès non autorisé. Toute personne agissant sous l'autorité du responsable du traitement, y compris un sous-traitant, ne doit traiter les données que sur instructions du responsable.

5) **Droits d'accès, de rectification, d'effacement et d'opposition**

Comme le prévoit l'article 12 de la directive 95/46/CE, la personne concernée doit avoir le droit d'accéder à toutes les données traitées qui la concernent et le cas échéant, d'obtenir leur rectification, leur effacement ou leur verrouillage lorsqu'il apparaît que leur traitement ne respecte pas les principes fixés dans le présent appendice, notamment parce que ces données sont incomplètes ou inexactes. Elle doit également être en mesure de s'opposer au traitement des données la concernant pour des raisons impérieuses et légitimes concernant sa situation personnelle.

6) **Restrictions aux transferts ultérieurs**

Les transferts ultérieurs de données à caractère personnel effectués par l'importateur de données vers un autre responsable du traitement établi dans un pays tiers n'offrant pas un niveau de protection adéquat ou non couverts par une décision de la Commission adoptée conformément à l'article 25, paragraphe 6, de la directive *95/46/CE* ne peuvent être autorisés que si :

a) les personnes concernées ont, dans le cas de catégories spéciales de données, indubitablement accepté le transfert ultérieur ou, dans les autres cas, la possibilité de s'y opposer.

Les informations minimales à fournir aux personnes concernées doivent contenir dans un langage qui leur soit compréhensible :

— l'objectif du transfert ultérieur ;
— l'identification de l'exportateur de données établi dans la Communauté ;
— les catégories des destinataires ultérieurs des données et les pays de destination, et;

— une remarque expliquant qu'après le transfert ultérieur, les données peuvent être traitées par un responsable du traitement établi dans un pays qui ne présente pas un niveau approprié de protection de la vie privée des personnes ;

ou

b) l'exportateur de données et l'importateur de données acceptent les clauses d'un autre responsable du traitement qui devient alors partie aux clauses et souscrit aux mêmes obligations que l'importateur de données.

7) Catégories particulières de données

Lorsque des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé et à la vie sexuelle et des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté sont traitées, des mesures de protection supplémentaires doivent être prévues au sens de la directive 95/46/CE, notamment des mesures de sécurité appropriées telles que procéder à un cryptage approfondi pour la transmission ou répertorier l'accès aux données sensibles.

8) Marketing direct

Lorsque des données sont traitées à des fins de marketing direct, des procédures efficaces doivent exister, permettant à la personne concernée de « s'opposer » à ce que les données la concernant soient, à un moment ou à un autre, utilisées à une telle fin.

9) Décisions individuelles automatisées

Les personnes concernées ont le droit de ne pas être soumises à une décision prise uniquement sur la base du traitement automatisé de données, à moins que d'autres mesures ne soient prises pour sauvegarder les intérêts légitimes de la personne comme le prévoit l'article 15, paragraphe 2, de la directive 95/46/CE. Lorsque la finalité du transfert est la prise d'une décision automatisée, au sens de l'article 15 de la directive 95/46/CE qui produit des effets juridiques à l'égard de la personne ou qui affecte de manière significative, et qui est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc, la personne doit avoir le droit de connaître la logique qui sous-tend cette décision.

APPENDICE 3 aux clauses contractuelles types

Principes obligatoires de protection des données visés au paragraphe 2 de la clause 5 (b)

1) Limitation des transferts à une finalité spécifique

Les données ne doivent être traitées et utilisées ou communiquées ultérieurement que pour les finalités spécifiques indiquées dans l'appendice 1 aux présentes clauses. Elles ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles sont transférées.

2) **Droits d'accès, de rectification, d'effacement et d'opposition** Comme le prévoit l'article 12 de la directive 95/46/CE, la personne concernée doit avoir le droit d'accéder à toutes les données traitées qui la concernent et le cas échéant, d'obtenir leur rectification, leur effacement ou leur verrouillage lorsqu'il apparaît que leur traitement ne respecte pas les principes fixés dans le présent appendice parce que les données sont incomplètes ou inexactes. Elle doit également être en mesure de s'opposer au traitement des données la concernant pour des raisons impérieuses et légitimes concernant sa situation personnelle.

3) **Restrictions aux transferts ultérieurs**

Les transferts ultérieurs de données à caractère personnel effectués par l'importateur de données vers un autre responsable du traitement établi dans un pays tiers n'offrant pas un niveau de protection adéquat ou non couverts par une décision de la Commission adoptée conformément à l'article 25, paragraphe 6, de la directive 95/46/CE ne peuvent être autorisés que si :

a) les personnes concernées ont dans le cas de catégories spéciales de don nées indubitablement accepté le transfert ultérieur ou, dans les autres cas, la possibi lité de s'y opposer.

Les informations minimales à fournir aux personnes concernées doivent contenir dans un langage qui leur soit compréhensible :

— l'objectif du transfert ultérieur ;
— l'identification de l'exportateur de données établi dans la Communauté ;
— les catégories des destinataires ultérieurs des données et les pays de destination, et;
— une remarque expliquant qu'après le transfert ultérieur, les données peuvent être traitées par un responsable du traitement établi dans un pays qui ne présente pas un niveau approprié de protection de la vie privée des personnes ;

ou ;

b) l'exportateur de données et l'importateur de données acceptent les clau ses d'un autre responsable du traitement qui devient alors partie aux clauses et sous crit aux mêmes obligations que l'importateur de données.

DÉCISION DE LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES DU 27 DÉCEMBRE 2001 RELATIVE AUX CLAUSES CONTRACTUELLES TYPES POUR LE TRANSFERT DE DONNÉES À cARACTÈRE PERSONNEL VERS DES SOUS-TRAITANTS ÉTABLIS DANS DES PAYS TIERS EN VERTU DE LA DIRECTIVE 95/46/CE[1] [notifiée sous le numéro C (2001) 4540]

(Texte présentant de l'intérêt pour l'EEE)

La Commission des communautés européennes ;

vu le traité instituant la Communauté européenne ;

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2], et notamment son article 26, paragraphe 4 ;

considérant ce qui suit :

(1) Conformément à la directive 95/46/CE, les États membres sont tenus de veiller à ce qu'un transfert de données à caractère personnel vers un pays tiers n'ait lieu que si le pays en question assure un niveau de protection adéquat des données et si les lois des États membres, qui sont conformes aux autres dispositions de la direc tive, sont respectées avant le transfert.

---

[1] JO L 6 du 10 janvier 2002, p. 52

[2] JO L 281 du 23 novembre 1995, p. 31.

(2) Toutefois, l'article 26, paragraphe 2, de la directive 95/46/CE prévoit que les États membres peuvent autoriser, sous certaines garanties, un transfert, ou un ensemble de transferts, de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat. Ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

(3) Conformément à la directive 95/46/CE, le niveau de protection des données doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel instauré au titre de ladite directive[1] a publié des lignes directrices afin de faciliter l'évaluation[2].

(4) Les clauses contractuelles types ne concernent que la protection des données et l'exportateur et l'importateur sont libres d'inclure d'autres clauses à caractère commercial qu'ils jugent pertinentes pour le contrat à condition qu'elles ne contredisent pas les clauses contractuelles types.

(5) La présente décision ne doit pas affecter les autorisations nationales que les États membres peuvent délivrer conformément aux dispositions nationales mettant en œuvre l'article 26, paragraphe 2, de la directive 95/46/CE. La présente déci sion a pour seul effet d'obliger les États membres à ne pas refuser de reconnaître que les clauses contractuelles qui y figurent offrent des garanties adéquates et elle n'a donc aucun effet sur d'autres clauses contractuelles.

(6) Le champ d'application de la présente décision se limite à établir que les clauses qu'elle énonce peuvent être utilisées par un responsable du traitement de données établi dans la Communauté pour offrir des garanties adéquates, au sens de l'article 26, paragraphe 2, de la directive 95/46/CE, pour le transfert de données à caractère personnel vers un sous-traitant établi dans un pays tiers.

(7) La présente décision doit mettre en oeuvre l'obligation prévue à l'article 17, paragraphe 3, de la directive 95/46/CE et n'affecte pas le contenu d'un contrat ou acte juridique établi conformément à cette disposition. Toutefois, certaines clau ses contractuelles types, relatives en particulier aux obligations de l'exportateur de données, doivent être incluses dans le but d'accroître la clarté en ce qui concerne les dispositions qui peuvent être introduites dans un contrat entre un responsable du trai tement des données et un sous-traitant.

(8) Les autorités de contrôle des États membres jouent un rôle-clé dans ce mé canisme contractuel en garantissant la protection adéquate des données à caractère personnel après le transfert. Dans les cas exceptionnels où les exportateurs de don nées refusent ou ne sont pas en mesure d'instruire convenablement l'importateur de données et où il existe un risque imminent de dommage grave pour les personnes

[1] L'adresse Internet du groupe de travail est la suivante : http://www.europa.eu.int/comm/internaLmarket /fr/dataprot/wpdocs/index.htm

[2] WP 4 (5020/97) « Premières orientations relatives aux transferts de données personnelles vers des pays tiers — Méthodes possibles d'évaluation du caractère adéquat de la protection », document de réflexion adopté par le groupe de travail le 26 juin 1997.
WP 7 (5057/97) « Évaluation des codes d'autoréglementation sectoriels : quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers ? », document de travail adopté par le groupe de travail le 14 janvier 1998.
WP 9 (5005/98) « Vues préliminaires sur le recours à des dispositions contractuelles dans le cadre de transferts de données à caractère personnel vers des pays tiers », document de travail adopté par le groupe de travail le 22 avril 1998.
WP 12 : « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données », document adopté par le groupe de travail le 24 juillet 1998 et disponible sur le site Web « http://www.europa.eu.int/comm/internal_rnarket/en/dataprot/wpdocs/wpl 2fr.pdf » de la Commission européenne.

concernées, les clauses contractuelles types doivent permettre aux autorités de contrôle de soumettre les importateurs de données à des vérifications et, lorsque cela s'avère approprié, de prendre des décisions auxquelles ces derniers devront se plier. Les autorités de contrôle doivent avoir la faculté d'interdire ou de suspendre un transfert de données ou un ensemble de transferts basé sur les clauses contractuelles types dans les cas exceptionnels où il est établi qu'un transfert basé sur des termes contractuels risque d'altérer considérablement les garanties et les obligations offrant un niveau de protection adéquat à la personne concernée.

(9) À l'avenir, la Commission pourra également examiner si les clauses con tractuelles types pour le transfert de données à caractère personnel vers des sous-trai tants de données établis dans des pays tiers n'offrant pas un niveau adéquat de protection des données, présentées par des organisations commerciales ou d'autres parties concernées, offrent des garanties suffisantes conformément à l'article 26, pa ragraphe 2, de la directive 95/46/CE.

(10) La divulgation de données à caractère personnel à un sous-traitant de données établi en dehors de la Communauté constitue un échange international pro tégé en vertu du chapitre IV de la directive 95/46/CE. En conséquence, la présente décision ne couvre pas le transfert de données à caractère personnel effectué par des responsables du traitement établis dans la Communauté vers des responsables du traitement établis en dehors de la Communauté qui relèvent du champ d'application de la décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clau ses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE[1].

(11) Les clauses contractuelles types doivent prévoir les mesures techniques et d'organisation assurant un niveau de sécurité adapté aux risques liés *au* traitement et à la nature des données à protéger que doit mettre en œuvre un sous-traitant établi dans un pays tiers n'offrant pas un niveau de protection adéquat. Les parties doivent prévoir dans le contrat les mesures techniques et d'organisation qui, eu égard au droit applicable à la protection des données, au niveau technologique et au coût de mise en œuvre, sont nécessaires pour protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divul gation ou un accès non autorisé ou toute autre forme illicite de traitement.

(12) Afin de faciliter les flux de données provenant de la Communauté, il est souhaitable que les sous-traitants offrant des services de traitement des données à plusieurs responsables du traitement des données de la Communauté soient autorisés à appliquer les mêmes mesures techniques et d'organisation liées à la sécurité, quel que soit l'État membre d'où provient le transfert de données, notamment dans les cas où l'importateur de données reçoit, pour un traitement ultérieur, des données originaires de différents établissements de l'exportateur de données dans la Communauté.

(13) Il convient de définir les informations minimales que les parties doivent prévoir dans le contrat relatif au transfert. Les États membres doivent conserver la fa culté de spécifier les informations que les parties doivent fournir. L'application de la présente décision doit être évaluée à la lumière de l'expérience acquise.

(14) L'importateur de données doit traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et selon ses instruc tions et les obligations incluses dans les clauses. En particulier, l'importateur de don nées ne doit divulguer les données à caractère personnel à un tiers que conformément à certaines conditions. L'exportateur de données doit charger l'impor-

[1] JO L 181 du 4 juillet 2001, p. 19.

tateur de données, pendant la durée des services de traitement des données, de traiter les données conformément à ses instructions, au droit applicable à la protection des données et aux obligations contenues dans les clauses. Le transfert de données à caractère personnel vers des sous-traitants établis en dehors de la Communauté n'enlève rien au fait que les activités de traitement doivent être régies en tout état de cause par le droit applicable à la protection des données.

(15) Les clauses contractuelles types doivent être exécutoires non seulement par les organisations parties au contrat mais également par les personnes concer nées, en particulier lorsque ces dernières subissent un dommage en raison d'une rup ture du contrat.

(16) La personne concernée doit avoir le droit d'exercer un recours et, lorsque cela s'avère approprié, d'obtenir réparation de l'exportateur de données qui est le responsable du traitement des données à caractère personnel transférées. À titre exceptionnel, la personne concernée doit aussi avoir le droit d'exercer un re cours et, lorsque cela s'avère approprié, d'obtenir réparation de l'importateur de données pour manquement par l'importateur de données à l'une ou à l'autre de ses obligations visées à la clause 3, deuxième alinéa, dans les cas où l'exportateur de données amatériellement disparu ou a cessé d'exister en droit ou est devenu insol vable.

(17) Si un litige entre la personne concernée qui invoque la clause du tiers bénéficiaire et l'importateur de données n'est pas résolu à l'amiable, l'importateur de données doit convenir de proposer à la personne concernée de choisir entre la médiation, l'arbitrage et la procédure judiciaire. La personne concernée aura réelle ment le choix dans la mesure où elle pourra disposer de systèmes de médiation et d'arbitrage fiables et reconnus. La médiation par les autorités de contrôle de la pro tection des données de l'État membre dans lequel est établi l'exportateur de données doit être une option lorsqu'elles fournissent un tel service.

(18) Le contrat doit être régi par le droit de l'Etat membre dans lequel l'ex portateur de données est établi et qui permet à un tiers bénéficiaire de faire exécuter un contrat. Les personnes concernées devront pouvoir être représentées par des asso ciations ou d'autres organismes si elles le souhaitent et si le droit national l'autorise.

(19) Le groupe de protection des personnes à l'égard du traitement des don nées à caractère personnel institué en vertu de l'article 29 de la directive 95/46/CE a émis un avis sur le niveau de protection prévu par les clauses contractuelles types annexées à la présente décision. Cet avis a été pris en considération dans la prépa ration de la présente décision[1].

(20) Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué en vertu de l'article 31 de la directive 95/46/CE ;

A arrêté la présente décision :

Article premier

Les clauses contractuelles types figurant en annexe sont considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des li bertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants comme l'exige l'article 26, paragraphe 2, de la directive 95/46/CE.

[1] Avis n° 7/2001 adopté par le groupe de travail le 13.9 2001 (DG MARKT .....), disponible sur le site Internet « Europa » de la Commission européenne.

Article 2

La présente décision concerne uniquement le caractère adéquat de la protection fournie par les clauses contractuelles types figurant en annexe pour le transfert de données à caractère personnel. Elle n'affecte pas l'application d'autres dispositions nationales mettant en œuvre la directive 95/46/CE qui se rapportent au traitement de données à caractère personnel dans les États membres.

La présente décision s'applique au transfert de données à caractère personnel par des responsables du traitement établis dans la Communauté à des destinataires établis en dehors du territoire de la Communauté qui agissent exclusivement en tant que sous-traitants.

Article 3

1 — Aux fins de la présente décision :
a) les définitions contenues dans la directive 95/46/CE s'appliquent ;
b) les « catégories particulières de données » sont les données visées à l'article 8 de ladite directive ;
c) l'« autorité de contrôle » est l'autorité visée à l'article 28 de ladite directive ;
d) l'« exportateur de données » est le responsable du traitement qui transfère les don nées à caractère personnel ;
e) l'« importateur de données » est le sous-traitant établi dans un pays tiers qui ac cepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux conditions de la présente décision et qui n'est pas soumis au système d'un pays tiers assurant une protection adéquate ;
f) le « droit applicable à la protection des données » est la législation protégeant les libertés et droits fondamentaux des personnes physiques, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans le pays où l'exportateur de données est établi ;
g) les « mesures techniques et d'organisation liées à la sécurité » sont les mesures destinées à protéger les données à caractère personnel contre une destruction for tuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non au torisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

Article 4

1 — Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées conformément aux chapitres II, III, V et VI de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour interdire ou suspendre les flux de données vers des pays tiers afin de protéger les individus à l'égard du traitement de leurs données à caractère personnel, et ce dans les cas où :
a) il est établi que le droit auquel l'importateur de données est soumis oblige ce der nier à déroger au droit applicable à la protection des données au-delà des limitations nécessaires dans une société démocratique pour l'une des raisons énoncées à l'ar ticle 13 de la directive 95/46/CE lorsque ces obligations risquent d'altérer considé rablement les garanties offertes par le droit applicable à la protection des données et les clauses contractuelles types, ou ;
b) une autorité compétente a établi que l'importateur de données n'a pas respecté les clauses contractuelles figurant en annexe, ou ;

c) il est fort probable que les clauses contractuelles types figurant en annexe ne sont pas ou ne seront pas respectées et que la poursuite au transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves.

2 — L'interdiction ou la suspension est levée dès que les raisons qui la motivaient disparaissent.

3 — Lorsque les États membres adoptent des mesures conformément aux paragraphes 1 et 2, ils en informent sans délai la Commission, qui transmet l'information aux autres États membres.

Article 5

La Commission évalue l'application de la présente décision, sur la base des informations disponibles, trois ans après sa notification aux États membres. Elle présente au comité institué au titre de l'article 31 de la directive 95/46/CE un rapport sur les constations effectuées. Le rapport comprend tout élément susceptible d'influer sur l'évaluation concernant le caractère adéquat des clauses contractuelles types figurant en annexe et tout élément indiquant que la présente décision est appliquée de manière discriminatoire.

Article 6

La présente décision s'applique à partir du 3 avril 2002.

Article 7

Les Etats membres sont destinataires de la présente décision.

ANNEXE
Clauses contractuelles types (« Sous-traitants »)

Aux fins de l'article 26, paragraphe 2, de la directive 95/46/CE pour le transfert des données à caractère personnel vers des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données

Nom *de l'organisation exportant les données* : .....
Adresse : **.....**

***Téléphone* :.....*Télécopieur :*.....**
***Courrier électronique* : .....**
Autres informations nécessaires pour *identifier l'organisation* : .....
(ci-après dénommée « **l'exportateur** de données »)

d'une part, et

Nom de *l'organisation important les données* : .....
Adresse : **.....**

Téléphone* :..... *Télécopieur : .....
***Courrier électronique* : .....**
Autres informations nécessaires pour identifier l'organisation : .....
(ci-après dénommée « **l'importateur** de données »)

d'autre part,

Sont convenus des clauses contractuelles suivantes (ci-après dénommées « les **clauses** ») afin d'offrir des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes lors du transfert, par l'exportateur de données vers l'importateur de données, des données à caractère personnel visées à l'appendice 1.

Clause première
Définitions

Au sens des clauses :

a) « ***données à caractère personnel*** », « ***catégories particulières de données*** », « ***traiter/traitement*** », « ***responsable du traitement*** », « ***sous-traitant*** », « ***personne concernée*** » et « ***autorité de contrôle*** » ont la même signification que dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommée « la directive »)[1] ;

b) « ***l'exportateur de données*** » est le responsable du traitement qui transfère les données à caractère personnel ;

c) « l'***importateur de données*** » est le sous-traitant qui accepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux termes des présentes clauses et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate.

d) le « *droit applicable à la protection des données* » est la législation protégeant les libertés et droits fondamentaux des personnes physiques, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans le pays où l'exportateur de données est établi.

e) les « ***mesures techniques et d'organisation liées à la sécurité*** » sont les mesures destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

Clause 2
Détails du transfert

Les détails du transfert et, notamment, les catégories particulières de données à caractère personnel, sont spécifiés dans l'appendice 1 qui fait partie intégrante des clauses.

Clause 3
Clause du tiers bénéficiaire

La personne concernée peut faire appliquer contre l'exportateur de données la présente clause, ainsi que la clause 4, points b) à h), la clause 5, points a) à, e) et g), la clause 6, points 1) et 2), la clause 7, la clause 8, point 2), et les clauses 9, 10 et 11 en tant que tiers bénéficiaire.

La personne concernée peut faire appliquer contre l'importateur de données la présente clause, la clause 5, points a) à e), et g), la clause 6, points 1) et 2), la clause 7, la clause 8, point 2), et les clauses 9, 10 et 11 dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit.

Les parties ne s'opposent pas à ce que la personne concernée soit représentée par une association ou un autre organisme si elle en exprime le souhait et si le droit national le permet.

[1] Les parties peuvent reprendre, dans la présente *clause,* les définitions et les significations de la directive 95/46/CE si elles estiment qu'il est préférable que le contrat soit autonome.

Clause 4

Obligations de l'exportateur de données

L'exportateur de données accepte et garantit ce qui suit :

a) le traitement, y compris le transfert proprement dit des données à caractère person nel, a été et continuera d'être effectué conformément aux dispositions pertinentes du droit applicable à la protection des données (et, le cas échéant, a été notifié aux au torités compétentes de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes audit État ;

b) il a chargé, et chargera pendant toute la durée des services de traitement de don nées à caractère personnel, l'importateur de données de traiter les données à carac tère personnel transférées pour le compte exclusif de l'exportateur de données et conformément au droit applicable à la protection des données et aux présentes clau ses ;

cj l'importateur de données offre suffisamment de garanties compte tenu des mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 du pré-sent contrat ;

d) après l'évaluation des exigences du droit applicable à la protection des données, les mesures de sécurité sont adéquates pour protéger les données à caractère person nel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une di vulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et elles assurent un niveau de sécurité adapté aux risques liés au traitement et à la na ture des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre ;

e) il veillera au respect des mesures de sécurité ;

f) si le transfert porte sur des catégories particulières de données, la personne concernée a été informée ou sera informée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat ;

g) il accepte de transmettre la notification reçue de l'importateur de données confor mément à la clause 5, point b), à l'autorité de contrôle de la protection des données s'il décide de poursuivre le transfert ou de lever sa suspension ;

h) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des clauses figurant dans la présente annexe, à l'exception de l'appendice 2 qui sera remplacé par une description sommaire des mesures de sécurité.

Clause 5

Obligations de l'importateur de données[1]

L'importateur de données accepte et garantit ce qui suit :

a) il traitera les données à caractère personnel pour le compte exclusif de l'exporta-teur de données, conformément aux instructions de ce dernier et aux clauses ; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'infor-

[1] Les exigences impératives de la législation nationale le concernant et qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique pour l'un des intérêts énoncés a l'article 13 de la directive 95/46/CE, c'est-à-dire si elles constituent une mesure nécessaire pour sauvegarder la sûreté de l'Etat ; la défense ; la sécurité publique ; la prévention, la recherche, la détection et la poursuite d'infrac-tions pénales ou de manquements à la déontologie dans le cas de professions réglementées ; un intérêt économique ou financier important d'un État membre ou la protection de la personne concernée ou des droits et libertés d'autrui, ne vont pas à l'encontre des clauses contractuelles types. Parmi les exemples de ces exigences impératives qui ne vont **pas** au-delà de celles qui sont nécessaires dans une société démo-cratique figurent, notamment, les sanctions reconnues sur le plan international, les obligations de déclara-tion fiscale et les obligations de déclaration de lutte contre le blanchiment des capitaux.

mer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat ;
b) il n'a aucune raison de croire que la législation le concernant l'empêche de rem plir les instructions données par l'exportateur de données et ses obligations prévues par le contrat et, en cas de modification de cette législation susceptible d'avoir des conséquences négatives importantes sur les garanties et les obligations prévues par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat ;
c) il a mis en oeuvre les mesures techniques et d'organisation liées à la sécurité spéci fiées dans l'appendice 2 avant de traiter les données à caractère personnel transfé rées ;
d) il communiquera sans retard à l'exportateur de données :
i) toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité responsable du maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction prévue par le droit pénal afin de préserver la confidentialité d'une enquête de police, ii) tout accès fortuit ou non autorisé et,
iii) toute demande reçue directement des personnes concernées sans y répondre, sauf autorisation contraire ;
e) il traitera de manière appropriée et en temps opportun toutes les demandes de ren seignements émanant de l'exportateur de données relatives au traitement effectué par ses soins des données à caractère personnel qui font l'objet du transfert et se ran gera à l'avis de l'autorité de contrôle en ce qui concerne le traitement des données transférées ;
f) à la demande de l'exportateur de données, il soumettra ses moyens de traitement de données à une vérification des activités de traitement couvertes par les clauses qui sera effectuée par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, sou mis à une obligation de secret et choisis par l'exportateur de données, le cas échéant, avec l'accord de l'autorité de contrôle ;
g) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des clauses figurant dans la présente annexe, à l'exception de l'appendice 2 qui sera remplacé par une description sommaire des mesures de sécurité, dans les cas où la personne concernée ne peut pas obtenir une copie auprès de l'exportateur de données.

Clause 6
Responsabilité

1 — Les parties conviennent qu'une personne concernée ayant subi un dom mage du fait d'une violation des dispositions visées à la clause 3 a le droit d'obtenir de l'exportateur de données réparation du préjudice subi.

2 — Si une personne concernée est empêchée d'intenter l'action visée au pa ragraphe 1 contre l'exportateur de données pour manquement par l'importateur de données à l'une ou à l'autre de ses obligations visées à la clause 3, parce que l'ex portateur de données a matériellement disparu ou a cessé d'exister en droit ou est de venu insolvable, l'importateur de données accepte que la personne concernée dépose une plainte à son encontre comme s'il était l'exportateur de données.

3 — Les parties conviennent que si l'une d'entre elles est tenue pour respon sable d'une violation des clauses commise par l'autre partie, dans la mesure où celle-ci est responsable, elle dédommagera la première partie de tout coût, charge,

dommage, dépense ou perte encourue par cette première partie. Le dédommagement dépend :
a) du délai dans lequel l'exportateur de données communique la plainte à l'importateur de données et ;
b) de la possibilité donnée à l'importateur de données de coopérer avec l'exportateur de données à la défense et au règlement de la plainte[1].

Clause 7
Médiation et juridiction

1 — L'importateur de données convient que si, en vertu des clauses, la personne concernée invoque à son encontre le droit du tiers bénéficiaire et/ou demande réparation du préjudice subi, il acceptera la décision de la personne concernée :
a) de soumettre le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle ;
b) de porter le litige devant les tribunaux de **l'État** membre dans lequel l'exportateur de données est établi.

2 — L'importateur de données convient que, en accord avec la personne concernée, le règlement d'un litige spécifique peut être porté devant un organe d'arbitrage si l'importateur de données est établi dans un pays qui a ratifié la convention de New York sur la reconnaissance et l'exécution des sentences arbitrales.

3 — Les parties conviennent que le choix fait par la personne concernée ne remettra pas en cause le droit procédural ou matériel de cette dernière d'obtenir réparation conformément à d'autres dispositions du droit national ou international.

Clause 8
Coopération avec les autorités de contrôle

1 — L'exportateur de données convient de déposer une copie du présent contrat auprès de l'autorité de contrôle si celle-ci l'exige ou si ce dépôt est prévu par le droit applicable à la protection des données.

2 — Les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications auprès de l'importateur de données dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées par l'autorité de contrôle auprès de l'exportateur de données conformément au droit applicable à la protection des données.

Clause 9
Droit applicable

Les clauses sont régies par le droit de l'Etat membre dans lequel l'exportateur de données est établi, à savoir .....

Clause 10
Modification du contrat

Les parties s'engagent à ne pas modifier les termes des clauses.

Clause 11
Obligation après la résiliation des services de traitement des données à caractère personnel

1 — Les parties conviennent qu'au terme des services de traitement des données, l'importateur de données restituera à l'exportateur de données, et à la convenance

[1] Le paragraphe 3 est facultatif.

de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies ou détruira ces données et en apportera la preuve à l'exportateur de données, à moins que la législation imposée à l'importateur de données l'empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, l'importateur garantit qu'il assurera la confidentialité des données à caractère personnel transférées et qu'il ne traitera plus activement ces données.

2 — L'importateur de données garantit que, si l'exportateur de données et/ou l'autorité de contrôle le demandent, il soumettra ses moyens de traitement de données à une vérification des mesures visées au paragraphe 1.

Au nom de l'exportateur de données :

Nom (écrit en toutes lettres) : .....
Fonction : .....
Adresse : .....
Autres informations nécessaires pour rendre le contrat contraignant (le cas échéant) :
…….
Signature : .....
(sceau de l'organisation)

Au nom de l'importateur de données :

Nom (écrit en toutes lettres) : .....
Fonction : .....
Adresse : .....
Autres informations nécessaires pour rendre le contrat contraignant (le cas échéant) :
…….
Signature : .....
(sceau de l'organisation)

APPENDICE 1 des clauses contractuelles types

Le présent appendice fait partie des clauses et doit être complété et signé par les parties

(* Les États membres peuvent compléter ou préciser, selon leurs procédures nationales, toute information supplémentaire devant éventuellement être incluse dans le présent appendice)

Exportateur de données

L'exportateur de données est *(veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert) :*

……
……

Importateur de données

L'importateur de données est *(veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert) :*

……
……

Personnes concernées

Les données à caractère personnel transférées ont trait aux catégories suivantes de personnes concernées *(veuillez préciser)* :

……
……..

Catégories de données

Les données à caractère personnel transférées concernent les catégories suivantes de données *(veuillez préciser)* :

……
……

Catégories particulières de données (le cas échéant)

Les données à caractère personnel transférées concernent les catégories particulières de données suivantes *(veuillez préciser) :*

……
……..

Traitement

Les données à caractère personnel transférées seront soumises aux activités de traitement de base suivantes *(veuillez préciser) :*

……
……

EXPORTATEUR DE DONNÉES IMPORTATEUR DE DONNÉES

Nom .....

Signature autorisée .....

APPENDICE 2 des clauses contractuelles types

Le présent appendice fait partie des clauses et doit être rempli et signé par les parties.

Description des mesures techniques et d'organisation liées à la sécurité mises en oeuvre par l'importateur de données conformément aux clauses 4, point d), et 5, point c) (ou document/législation jointe) :

……
……
……
……

Annexe 10

Travaux du groupe article 29

AVIS 10/2001 SUR LA NÉCESSITÉ D'UNE APPROCHE ÉQUILIBRÉE DANS LA LUTTE CONTRE LE TERRORISME Adopté le 14 décembre 2001

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel

créé par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1];

vu les articles 29 et 30 paragraphes 1 et 3 de cette directive ;

vu son règlement intérieur, et notamment ses articles 12 et 14 ;

a adopté l'AVIS suivant :

Les tragiques attaques terroristes contre les Etats-Unis ont mis en évidence la nécessité pour les sociétés démocratiques de s'engager dans une lutte contre le terrorisme. Cet objectif est un élément constitutif, à la fois nécessaire et précieux, des sociétés démocratiques. Dans cette lutte, certaines conditions faisant également partie des fondements de nos sociétés démocratiques doivent être respectées.

Dans ce contexte particulier, diverses mesures sont actuellement examinées tant au niveau communautaire[2] qu'au niveau des États membres. Certaines sont très innovantes, d'autres le sont moins et constituent simplement une mise à jour de projets existants qui reçoivent un intérêt renouvelé. Dans de nombreux cas, ces mesures couvrent des domaines dépassant le cadre de la lutte contre le terrorisme. On observe une prolifération de l'utilisation de systèmes d'identification, et plus généralement, de collectes de données à caractère personnel à travers l'emploi, par exemple, de la biométrie. De plus, on constate une augmentation de la criminalisation de certains comportements liés à la société de l'information — la « cybercriminalité » — comme l'intrusion dans les systèmes d'information, mais aussi la reproduction de travaux protégés par les droits d'auteur[3]. Les définitions de ces délits sont souvent générales, et suscitent par conséquent des questions à l'égard des principes fondamentaux de la sécurité juridique et de la légalité des infractions et des sanctions[4]. D'autre part, les mesures procédurales existantes légitimant l'intrusion des pouvoirs publics dans la vie privée des individus sont renforcées et de nouvelles initiatives contestables sont examinées, voire adoptées. Cela ne concerne pas seulement les écoutes téléphoniques mais aussi d'autres mesures telles que la conservation préalable et généralisée des données des télécommunications par les fournisseurs et opérateurs de services de communications électroniques, l'adoption de mesures permettant la surveillance en « temps réel » des citoyens, l'abandon du principe de la double incrimination comme condition d'échange de certaines données à caractère

---

1 *JO* n° L 281 du 23 novembre 1995, p. 31, disponible sur : http://europa.eu.mt/carnm/internal_market/en/dataprot/index.htrn

2 Voir notamment les conclusions du sommet européen Justice et Affaires intérieures du 20 septembre 2001, la « feuille de route » de l'Union européenne du 15 novembre 2001 suite aux attentats aux Etats-Unis (13880/1).

3 Aux États-Unis, le *Recording Industry Association of America* (RIAA) a essayé de faire adopter un amende ment lors des discussions autour du « *Patriot Act* ». Cet amendement aurait conféré à ce secteur l'autorisa tion juridique de s'introduire dans les systèmes informatiques afin d'identifier les personnes coupables d'infractions à la législation sur les droits d'auteur.

4 Voir la Convention du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre

personnel concernant les criminels, le partage de données à caractère personnel à des fins diverses telles que la lutte contre la criminalité, l'immigration, le contre-espionnage et le transfert prématuré de données à caractère personnel vers des pays tiers. De tels transferts peuvent être particulièrement dangereux si le pays destinataire n'offre pas de garanties suffisantes de protection des données.

Toutes ces mesures ont un impact direct ou indirect sur la protection des données à caractère personnel. Le groupe a présenté plusieurs avis sur des questions apparentées[1], en ayant pleine connaissance du grave problème du terrorisme, un phénomène que connaît, malheureusement, l'Europe depuis un certain temps.

Dans ce contexte, le groupe de travail rappelle l'engagement de nos sociétés démocratiques à garantir le respect des libertés et droits fondamentaux de la personne. Les droits de la personne à la protection des données à caractère personnel constituent une partie de ces libertés et droits fondamentaux[2]. Les directives de la Communauté sur la protection des données à caractère personnel (directives 95/46/CE et 97/66/CE font partie de cet engagement[3]. Ces directives ont pour objet de garantir le respect des libertés et droits Fondamentaux, en particulier le droit au respect de la vie privée à l'égard du traitement des données à caractère personnel et de contribuer au respect des droits protégés par la Convention européenne des droits de l'homme, notamment son article 8. Toutes ces dispositions prévoient des exceptions pour lutter contre la criminalité qui doivent cependant respecter certaines conditions.

Le groupe de travail souligne en particulier la nécessité de prendre en compte l'impact à long terme d'actions urgentes rapidement mises en application ou envisagées en ce moment. Cette réflexion à long terme est d'autant plus nécessaire si l'on considère que le terrorisme n'est pas un phénomène nouveau et ne peut être qualifié de phénomène temporaire. Le groupe souligne également l'obligation de respecter le principe de proportionnalité concernant toute mesure restreignant le droit fondamental au respect de la vie privée selon l'article 8 de la Convention européenne des droits de l'homme et la jurisprudence s'y rapportant. Cela implique, entre autres, l'obligation de démontrer que toute mesure prise correspond à un « besoin social impératif ». Les mesures qui sont simplement « utiles » ou « souhaitées » peuvent ne pas restreindre les libertés et droits fondamentaux. Le groupe de travail souligne donc la nécessité d'organiser un débat approfondi sur les actions de lutte contre le terrorisme, en analysant toutes leurs conséquences sur les libertés et droits fondamentaux des personnes et en refusant notamment l'amalgame entre la lutte

---

1 Voir notamment le document de travail « traitement des données à caractère personnel sur l'Internet » du 23 février 1999, recommandations 1 /99 sur le « traitement invisible et automatique des données à caractère personnel sur l'Internet effectué par des moyens logiciels et matériels » et 2/99 concernant « le respect de la vie privée dans le contexte de l'interception des télécommunications » et 3/99 relative à « la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit », le document de travail « le respect de la vie privée sur Internet — une approche européenne intégrée sur la protection des données en ligne » du 21 novembre 2000, les avis 2/2000 concernant « le réexamen général du cadre juridique dans le domaine des télécommunications » et 7/2000 sur la « proposition de la Communication européenne d'une directive du Parlement européen et du Conseil concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 — COM (2000) 385 », l'avis 4/2001 sur « le projet de convention du Conseil de l'Europe concernant la criminalité informatique » et l'avis 9/2001 sur la communication de la Commission intitulée « créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité ». Tous les documents sont disponibles sur : http://europa.eu.int/comm/internal_marker/en/dataprot/index.htm

2 Voir en particulier l'article 8 de la Charte des droits fondamentaux de l'Union européenne, ainsi que la jurisprudence de la Cour européenne des Droits de l'homme dans les récentes affaires *Aman* du 16 février 2000 et *Rotaru* du 4 mai 2000.

3 Voir considérant 1,2, 10 et 11 de la directive 95/46/CE et considérant 2 de la directive *97/66/CE*.

contre le terrorisme réel et la lutte contre la criminalité en général, et en limitant également les mesures procédurales empiétant sur la vie privée à celles qui sont absolument nécessaires.

De plus, le groupe de travail rappelle que les mesures législatives limitant le droit des personnes au respect de la vie privée doivent être accessibles et prévisibles quant à leurs implications pour les personnes concernées. Cette exigence implique une législation suffisamment claire dans ses définitions des circonstances, de l'étendue et des modalités d'exercice des mesures d'intrusion. Les dispositions doivent être claires et détailler les circonstances dans lesquelles les pouvoirs publics sont autorisés à prendre des mesures limitant les droits fondamentaux. Elles devraient notamment spécifier où ces mesures peuvent être utilisées et devraient exclure toute surveillance générale ou préliminaire et offrir une protection contre les attaques arbitraires des pouvoirs publics[1].

Finalement, le groupe de travail s'inquiète de la tendance accrue à se représenter la protection des données à caractère personnel comme un obstacle à la lutte efficace contre le terrorisme. Le groupe de travail souhaite rappeler que les textes sur la protection des données (incluant les directives 95/46/CE et 97/66/CEE ainsi que l'article 8 de la charte des droits fondamentaux de l'Union européenne) d'une part ont pour objet de protéger les droits fondamentaux du citoyen et d'autre part, contiennent les exceptions nécessaires pour lutter contre la criminalité dans les limites autorisées par la Convention européenne des Droits de l'homme.

Les mesures contre le terrorisme ne devraient pas et n'ont pas besoin de réduire les niveaux de protection des droits fondamentaux qui caractérisent nos sociétés démocratiques. Un élément clé de la lutte contre le terrorisme doit consister à garantir la préservation des valeurs fondamentales qui sont la base de nos sociétés démocratiques et qui sont les valeurs mêmes, que ceux prônant l'usage de la violence cherchent à détruire.

Fait à Bruxelles, le 14 décembre 2001

Par le groupe de travail

Le Président

Stefano RODOTA

RECOMMANDATION CONCERNANT CERTAINES EXIGENCES MINIMALES POUR LA COLLECTE EN LIGNE DE DONNÉES À cARACTÈRE PERSONNEL DANS L'UNION EUROPÉENNE ADOPTÉE LE 17 MAI 2001

Le groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organisme communautaire indépendant et à caractère consultatif sur la protection des données et de la vie privée. Ses tâches sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE. Le secrétariat est assuré par : la Commission européenne, DG marché intérieur, fonctionnement et impact du marché intérieur. Coordination. Protection des données. Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussels — Belgique — Bureau : CI 00-6/136

[1] Voir notamment la jurisprudence de la Cour européenne des Droits de l'homme, dans les affaires *Chappell* (30 mars 1989, n° 152, point 56), *Malone* (2 août 1984, point 67 et 68), *Sunday Times* (26 avril 1979, point 49), Valenzuela Confreras (30 juillet 1998, point 46) et *Lambert* (24 août 1998).

Téléphone : ligne directe (+32-2) 295.72.58 ou 299.27.19, centrale 299.11.11. Fax: 296.80.10

Adresse Internet : http://europa.eu.int/comm/internal market/fr/media/dataprot/wpdocs/index.htm

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1];

vu l'article 29 et l'article 30, paragraphe 1, point a) et paragraphe 3 de ladite directive ;

vu son règlement intérieur et, en particulier, ses articles 12 et 14 ;

a adopté la présente recommandation :

I. Introduction

1 — Dans son document de travail intitulé « Le respect de la vie privée sur Internet — Une approche européenne intégrée de la protection des données en ligne » du 21 novembre 2000[2], le groupe de travail a souligné l'importance de veiller à ce que des moyens adéquats soient mis en place afin de garantir que les internautes disposent de toutes les informations nécessaires pour accorder, en toute connaissance de cause, leur confiance aux sites qu'ils consultent et effectuer, au besoin, certains choix conformément aux droits qui leur sont conférés par la législation européenne. Ceci est d'autant plus important que l'utilisation d'Internet multiplie les occasions de collecte de données à caractère personnel et, partant, les risques pour les libertés et droits fondamentaux des individus, en particulier leur vie privée. Dans son avis n° 4/2000 du 16 mai 2000 sur le niveau de protection offert par les « principes de la sphère de sécurité », le groupe de travail a invité la Commission à envisager en priorité la création d'un système de sécurité européen pour les sites Internet, fondé sur des critères communs d'évaluation de la protection des données pouvant être déterminés au niveau communautaire. La présente recommandation s'inscrit dans la continuité des deux documents susmentionnés. Elle a pour objet de contribuer à l'application efficace et homogène des dispositions nationales de mise en oeuvre des directives relatives à la protection des données à caractère personnel[3] en fournissant des indications concrètes sur la manière dont les règles définies dans ces directives doivent être appliquées aux traitements les plus couramment effectués via Internet. Ces traitements interviennent notamment lors d'un « premier contact » entre un internaute et un site Internet, que ce soit uniquement en vue de rechercher des informations ou de conclure une transaction commerciale étape par étape.

Les orientations ci-dessous concernent principalement la collecte de données à caractère personnel sur Internet et visent à énoncer les mesures concrètes à mettre en oeuvre par les différents acteurs afin de veiller à ce que les données soient traitées

---

1 *JO* n° L 281, du 23 novembre 1995, p. 31, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/fr/rnedia/dataprol/index.htrn

2 WP 37 (5063/00) : document de travail intitulé « Le respect de la vie privée sur Internet — Une approche européenne intégrée de la protection des données en ligne », adopte le 21 novembre 2000. Ce document est disponible à l'adresse suivante : hltp://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37fr.pdf

3 Directive *95/46/CE* du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la pro tection de la vie privée dans le secteur des télécommunications. Disponibles à l adresse suivante : http://europa.eu.int/comm/internal_market/fr/media/dataprot/law/index.htm

de manière licite et loyale (application des articles *6,7,* 10 et 11 de la directive 95/46/CE). Elles précisent notamment la nature des informations qui doivent être fournies aux utilisateurs et quand et comment elles doivent l'être, mais comprennent également des détails pratiques sur d'autres droits et obligations découlant des directives.

La présente recommandation vise donc essentiellement à apporter une aide pratique à la mise en œuvre des principes généraux de la directive. Le groupe de travail considère cette recommandation comme un premier pas vers la définition, au niveau européen, d'une série « minimale » d'obligations pouvant être aisément satisfaites par les responsables du traitement (à savoir les personnes physiques ou morales responsables du traitement des données à caractère personnel dans le cadre d'un site Internet)[1] qui gèrent des sites ; ces exigences seront, le cas échéant, complétées par des détails ou des sujets supplémentaires[2]. Il va sans dire que cela ne dispense pas les responsables du traitement de leur obligation de vérifier que leurs traitements sont conformes à toutes les exigences et conditions définies dans la législation nationale applicable et qu'ils sont donc licites.

Cette recommandation s'applique si le responsable du traitement est établi dans un des États membres de l'Union européenne. Dans ce cas, la législation nationale de l'État membre concerné s'applique au traitement des données à caractère personnel dans le cadre des activités de cet établissement. La recommandation s'applique également si le responsable du traitement n'est pas établi sur le territoire de la Communauté, mais recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire d'un État membre de l'UE. Le traitement est alors couvert par la législation nationale de l'Etat membre où se trouvent les installations ou moyens techniques[3].

2 — Pour réaliser cet objectif, la recommandation s'adresse en particulier :

---

1 À toutes fins utiles, l'article 2 de la directive 95/46/CE définit le responsable du traitement comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjoin tement avec d'autres, détermine-les finalités et les moyens du traitement de données a caractère person nel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ».

2 Les recommandations concrètes formulées dans le présent document représentent des exigences minima
les dans le sens qu'il en existe d'autres. Elles seront complétées à l'avenir par d'autres recommandations sur le traitement de données à caractère personnel plus sensibles, telles que celles liées à des sites sur la santé, à des sites adressés à des enfants ou à des services de portail. En ce qui concerne d'autres traite ments spécifiques, tels que la diffusion de données à caractère personnel sur un site ou l'enregistrement de données de trafic par des fournisseurs de services Internet ou des fournisseurs de services et de contenus Internet, voir les recommandations du groupe de travail dans le document mentionné à la note de bas de page n° 1 et d'autres avis pertinents adoptés par le groupe de travail, tels que : WP 25 (5085/99) : « Re commandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services Inter net pour le respect du droit », adoptée le 7 septembre 1999. WP 18 (5005/99) : « Recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications », adoptée le 3 mai 1999 et WP 17 (5093/98) : « Recommandation 1 /99 sur le traitement invisible et auto matique des données à caractère personnel sur Internet effectué par des moyens logiciels et matériels », adoptée le 23 février 1999. Tous ces documents sont disponibles à l'adresse indiquée à la note de bas de page n° 1.

3 Voir l'article 4, paragraphe 1, points a) et c) de la directive 95/46/CE. Ce point ne doit pas être confon du avec la question de savoir si les données à caractère personnel peuvent faire l'objet d'un transfert licite de l'UE vers un pays tiers. Cette question est traitée dans les articles 25 et 26 de la directive 95/46/CE et les décisions connexes de la Commission européenne concernant la reconnaissance d'un niveau adéquat de protection dans un pays tiers. Ainsi, si un site Internet américain a recours à des moyens situés dans l'UE pour collecter et traiter des données à caractère personnel, la législation du pays européen en ques tion s'appliquera aux opérations de collecte et de traitement, que l'entreprise soit considérée ou non comme offrant un niveau adéquat de protection, conformément à la décision de la Commission euro péenne relative à la sphère de sécurité. La question de savoir si un destinataire a souscrit aux principes de la sphère de sécurité ne sera pertinente que pour déterminer la licité des transferts ultérieurs des données à caractère personnel d'une entreprise établie dans l'UE vers l'entreprise en question.

— aux responsables du traitement collectant des données en ligne, en leur fournis sant un guide pratique recensant la série minimale de mesures concrètes à mettre en œuvre ;
— aux internautes afin qu'ils connaissent leurs droits et puissent les exercer ;
— aux organismes qui souhaitent délivrer un label attestant de la conformité des pro cédés de traitement utilisés avec les directives européennes de protection des don nées, en leur procurant les critères de référence nécessaires à l'octroi d'un tel label au regard des informations à fournir et de la collecte de données à caractère person nel. Il va sans dire qu'en plus de ces critères de référence, d'autres critères concer nant d'autres droits et obligations doivent être impérativement pris en compte pour l'octroi de labels. Le groupe de travail publiera ultérieurement un document complet sur cette question ; — aux autorités européennes chargées de la protection des don nées afin de leur fournir un outil de référence commun pour le contrôle du respect des dispositions nationales adoptées par les États membres en application des directives précitées.

3 — Le groupe de travail est en outre d'avis que cette recommandation doit servir de référence à l'élaboration de normes concernant les logiciels et le matériel destinés à la collecte et au traitement de données à caractère personnel sur Internet.

II. Recommandations concernant les informations à fournir lors de la collecte de données à caractère personnel sur le territoire des États membres de l'Union européenne

Quelles Informations doivent-elles être fournies à la personne concernée et à quel moment ?

4 — Toute collecte de données à caractère personnel auprès d'une personne via un site Internet suppose la fourniture préalable de certaines informations. En ter mes de contenu, le respect de cette obligation nécessite :

5 — d'indiquer l'identité et l'adresse physique et électronique du respon sable du traitement et, le cas échéant, celle du représentant désigné en application de l'article 4, paragraphe 2, de la directive ;

6 — d'indiquer clairement la (les) finalité (s) du traitement des données re cueillies par le responsable du traitement via un site. Par exemple, lorsque des don nées sont collectées tant pour l'exécution d'un contrat (abonnement Internet, commande d'un produit, etc.) que pour des opérations de prospection, le respon sable du traitement doit indiquer clairement ces deux finalités ;

7 — de signaler clairement le caractère obligatoire ou facultatif des informa tions à fournir.

Les informations obligatoires sont celles en l'absence desquelles le service demandé ne peut être réalisé. Le caractère obligatoire ou facultatif peut être indiqué, par exemple, par un astérisque renvoyant au caractère obligatoire des informations ou, à l'inverse, par l'ajout de la mention « facultatif » en marge des informations non obligatoires. Le fait que la personne concernée ne fournisse pas les informations facultatives ne peut en aucun cas lui être préjudiciable.

8 — de mentionner l'existence et les modalités d'exercice du droit de consentir ou de s'opposer, selon le cas, au traitement des données à caractère per sonnel[1] ainsi que des droits d'accès, de rectification et de suppression des don-

[1] Un traitement à des fins spécifiques n'est légitime que s'il repose sur une des raisons énumérées à l'article 7 de la directive 95/46/CE (notamment si la personne concernée a indubitablement donné son consentement, si le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, s'il

nées ; il convient d'indiquer la personne ou le service à contacter pour exercer ces droits ainsi que la possibilité de les exercer tant en ligne qu'à l'adresse physique du responsable du traitement ;

9 — d'indiquer les destinataires ou les catégories de destinataires des informations collectées. Les sites doivent préciser si les données recueillies seront communiquées à des tiers (partenaires commerciaux, filiales, etc., notamment), et à quelles fins (à des fins autres que la prestation du service demandé et à des fins de prospection[1] *8)*. Dans ce cas, les internautes doivent effectivement avoir la possibilité, en cochant une case, de s'opposer en ligne à la transmission des données à des fins autres que la prestation du service demandé. Le droit d'opposition pouvant être exercé à tout moment, la possibilité de l'exercer en ligne doit également figurer dans les informations fournies à la personne concernée. Conscient de l'intérêt de ne pas surcharger les écrans d'informations, le groupe de travail estime que l'absence de toute mention relative aux destinataires vaut engagement du responsable du traitement à ne pas communiquer les données collectées à des tiers dont le nom et les coordonnées ne sont pas précisés, sauf si l'identité du tiers est évidente et si la communication des données est indispensable à la prestation du service demandé par l'internaute et n'est effectuée qu'à cette fin ;

10 — lorsque les données sont destinées à être transférées par le responsable du traitement vers un pays tiers à l'Union européenne, de préciser si ce pays offre ou non un niveau de protection adéquat des personnes physiques à l'égard du traitement des données à caractère personnel au sens de l'article 25 de la directive *95/46/CE*. Dans ce cas, il est nécessaire de fournir des informations spécifiques concernant l'identité et les coordonnées des destinataires (adresse physique et/ou électronique)[2];

11 — de mentionner le nom et les coordonnées (adresse physique et électronique) du service ou de la personne chargés de répondre aux questions concernant la protection des données à caractère personnel ;

12 — d'indiquer clairement l'existence de procédés de collecte automatique des données, préalablement à toute collecte par un tel moyen[3];

En cas d'utilisation de tels procédés, les éléments d'information mentionnés dans le présent document doivent être communiqués à la personne concernée. En outre, cette dernière doit également être informée du nom de domaine du serveur du site transmettant les procédés de collecte automatique, de la finalité de ces procédés,

---

est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévale pas l'intérêt de la personne concernée). Le droit d'opposition (voir article 14) est accordé par les Etats membres dans au moins deux des cas visés à l'article 7, y compris le dernier susmentionné. La personne concernée a le droit, sauf en *cas* de disposition contraire du droit national, de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement. Le droit de s'opposer, sur demande et gratuitement, existe lorsque les données sont traitées à des fins de prospec ion. En outre, la personne concernée peut s'opposer gratuitement (une fois informée et dès la première fois) à ce que des données à caractère personnel soient communiquées à des tiers ou u ilisées pour le compte de tiers à des fins de prospection.

1 Les données ne peuvent être communiquées à des tiers que si la finalité prévue n'est pas incompatible avec celle pour laquelle les données ont été recueillies et repose sur un des cas énumérés à l'article 7, rendant le traitement légitime.

2 Des informations sur les décisions relatives au niveau adéquat de protection peuvent être consultées sur le site Internet de la Commission à l'adresse suivante : http://europa.eu.int/comm/internal_market/fr/media/dataprot/index.htm

3 Le traitement « invisible » et automatique des données à caractère personnel est soumis aux mêmes conditions et garanties que les autres types de traitement. Voir la recommandation 1 /99 du groupe de travail sur le traitement invisible et automatique des données à caractère personnel sur Internet effectués par des moyens logiciels et matériels (23 février 1999), disponible sur le site Internet mentionné à la note de bas de page n° 1.

de leur durée de validité, de l'éventuelle nécessité d'accepter ces procédés pour visiter le site, de la possibilité dont dispose tout internaute de s'opposer à leur utilisation ainsi que des conséquences de la désactivation de ces procédés. Lorsque d'autres responsables du traitement participent à la collecte de données à caractère personnel, la personne concernée doit être informée de l'identité de chacun d'entre eux ainsi que des différentes finalités du traitement poursuivies.

Les informations et la possibilité de s'opposer à la collecte doivent être communiquées avant la mise en œuvre des procédés automatiques qui connectent le PC de l'utilisateur à un autre site Internet (par exemple, lorsque l'utilisateur est automatiquement amené par un site à en contacter un autre afin de voir des publicités sous forme de bannières ; on évite ainsi que ce deuxième site ne collecte des données à l'insu de l'utilisateur).

Ainsi, si le serveur d'un responsable du traitement place Un cookie, il doit le signaler avant que le cookie ne soit envoyé sur le disque dur de l'internaute, en plus des informations automatiquement fournies par la technologie existante, qui se limite à indiquer le nom du site émetteur et la durée de validité du cookie[1];

13 — de faire état des mesures de sécurité garantissant l'authenticité du site ainsi que l'intégrité et la confidentialité des informations transmises sur le réseau, conformément à la législation nationale applicable[2];

14 — de fournir les informations dans toutes les langues utilisées sur le site et, en particulier, là où des données à caractère personnel sont collectées ;

15 — les responsables du traitement doivent s'assurer de la cohérence des informations contenues dans les différents « documents » qui engagent le site (ru brique « protection des données à caractère personnel », formulaires électroniques, texte relatif aux conditions générales de vente et autres communications commercia les).

Comment fournir les informations ?

16 — Le groupe de travail estime que les informations suivantes doivent ap paraître directement à l'écran avant la collecte afin de garantir le traitement loyal des données. Ces informations concernent :

— l'identité du responsable du traitement ;
— la (les) finalité (s) ;
— le caractère obligatoire ou facultatif des informations demandées ;
— les destinataires ou les catégories de destinataires des données recueillies ;
— l'existence d'un droit d'accès aux données et de rectification de ces données ;
— l'existence du droit de s'opposer à toute communication des données à des tiers à des fins autres que la prestation du service demandé et la procédure à suivre à cet égard (case à cocher, par exemple) ;
— les informations à fournir en cas d'utilisation de procédés de collecte automa tique ;
— le niveau de sécurité durant toutes les étapes du traitement, y compris la transmis sion via des réseaux, par exemple.

Dans ces cas, les informations doivent être fournies à l'écran de manière interactive.

[1] Si une organisation place un cookie via son propre site Internet et qu'elle seule peut accéder au contenu du cookie, aucune information supplémentaire ne doit être fournie sur son identité, à condition que l'orga nisation qui héberge le site ait déjà été identifiée de manière adéquate.

[2] Voir les règles spécifiques visées à l'article 17, paragraphe 1, et paragraphe 3, deuxième tiret, de la di rective 95/46/CE.

Si des procédés de collecte automatique sont utilisés, les informations correspondantes peuvent, si nécessaire, être affichées en mode fenêtre.

Quant aux informations relatives à la sécurité de la transmission des données du PC de l'utilisateur vers le site Internet, elles peuvent être formulées comme suit : « Vous entrez dans une session sécurisée » ou être automatiquement transmises par le navigateur, par exemple, par le biais d'icônes spécifiques (clé ou cadenas).

17 — Le groupe de travail considère en outre que des informations complètes sur la politique de protection des données (y compris les modalités d'exercice du droit d'accès) doivent être directement accessibles à partir de la page d'accueil du site ainsi que de tout endroit où des données à caractère personnel sont collectées en ligne. L'intitulé de la rubrique à cliquer doit être suffisamment mis en évidence, explicite et spécifique pour permettre à l'internaute de se faire une idée claire du contenu vers lequel il est renvoyé. Par exemple, il pourrait être précisé « Nous collectons et traitons des données à caractère personnel vous concernant. Pour plus d'informations, cliquer ici » ou « Protection des données à caractère personnel ». Le contenu des informations vers lesquelles l'internaute est dirigé doit également être suffisamment spécifique.

III. Recommandations relatives à la mise en œuvre d'autres droits et obligations

Le groupe de travail souhaite également attirer l'attention des destinataires de la présente recommandation sur certains autres droits des personnes et obligations des responsables du traitement qui découlent des directives et revêtent une importance particulière pour la collecte de données à caractère personnel sur des sites Internet. Le groupe de travail considère que les recommandations ci-dessous présentent, à l'instar des indications sur les informations à fournir, un intérêt pratique immédiat tant pour les responsables du traitement que pour les internautes.

18 — Seules les données nécessaires à la réalisation de la finalité prévue doivent être collectées.

19 — Il faut veiller à ce que les données soient traitées de manière légitime sur la base de l'un des critères énumérés à l'article 7 de la directive *95/46/CE.*

20 — Il convient d'assurer la mise en œuvre effective des droits d'accès et de rectification, qui doivent pouvoir s'exercer tant à l'adresse physique du responsable du traitement qu'en ligne. Des mesures de sécurité doivent être prises afin de garantir que seule la personne concernée puisse accéder en ligne aux informations qui la concernent.

21 — Il convient d'appliquer le principe de « finalité » selon lequel les don nées à caractère personnel ne doivent être utilisées que lorsque cela est nécessaire à une fin spécifique. En d'autres termes, les données à caractère personnel ne peuvent être utilisées que pour des finalités légitimes et la personne concernée doit rester ano nyme (article 6, paragraphe 1, point b) de la directive 95/46/CE). Ce principe est parfois qualifié de « principe de minimisation des données ».

22 — Dans un contexte identique à celui décrit au point 21, il doit être pos sible de consulter un site commercial de manière anonyme, c'est-à-dire sans que l'uti lisateur ne soit tenu de mentionner son nom, prénom, adresse électronique ou autres données d'identification. Cette possibilité de consultation anonyme doit être encou ragée. Lorsqu'un lien vers une personne est nécessaire, sans qu'une identification complète ne soit requise pour autant, l'utilisation de pseudonymes de toute sorte doit être proposée et acceptée.

En l'absence d'exigence juridique d'identification, l'utilisation de pseudonymes doit être encouragée et acceptée, même dans le cadre de certaines transactions. Un exemple est l'utilisation de pseudonymes dans les certificats pour les signatures électroniques (voir l'article 8 de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques).

23 — Il convient de déterminer une durée de conservation des données col lectées. Les données doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées (article 6 de la directive 95/46/CE et article 6 de la directive 97/66/CE).

24 — Les mesures nécessaires doivent être prises afin de garantir la sécurité des données lors du traitement, y compris lors de la transmission (par exemple, déter miner et restreindre le cercle de personnes ayant accès aux données, utiliser un cryp tage approfondi) (article 17 de la directive 95/46/CE).

25 — Lorsqu'un sous-traitant participe à l'hébergement d'un site Internet, par exemple, il convient de conclure un contrat le contraignant à prendre des mesu res de sécurité appropriées, conformément à la législation de l'État membre où il est situé, et à ne traiter les données à caractère personnel que suivant les instructions du responsable du traitement.

26 — Selon la loi nationale applicable, l'autorité de contrôle compétente doit être notifiée (lorsque le responsable du site est établi dans l'Union européenne ou qu'il y dispose d'un représentant). Le numéro d'enregistrement de la notification peut avantageusement figurer sous la rubrique du site consacrée à la protection des données.

27 — En cas de transfert vers un pays tiers n'assurant pas un niveau de pro tection adéquat, il faut veiller à ce que le transfert des données n'ait lieu que s'il est conforme à l'une des dérogations prévues à l'article 26 de la directive 95/46/CE. Dans ce cas, la personne concernée doit être informée des garanties adéquates exis tantes afin de rendre le transfert licite.

IV. Collecte d'adresses pour la prospection par courrier électronique et envoi de lettres d'informations

28 — En ce qui concerne la prospection par courrier électronique :

— Le groupe de travail insiste sur le fait que l'utilisation d'adresses électroni ques collectées dans des espaces publics d'Internet, tels que les groupes de discus sion, à l'insu de la personne concernée, est illicite. Ces adresses ne peuvent pas être utilisées à des fins autres que celle pour laquelle elles ont été diffusées, et surtout pas pour la prospection[1].

— Les adresses électroniques ne peuvent être utilisées à des fins de prospec tion que lorsqu'elles ont été collectées de manière loyale et licite. Une collecte loyale et licite suppose que les personnes concernées ont été informées de la possibilité de l'utilisation de ces données à des fins de prospection et mises en mesure de consentir

[1] Voir les documents WP 28 (5007/00) « Avis 1 /2000 sur certains aspects du commerce électronique relatifs à la protection des données », adopté le 3 février 2000, WP 29 (5009/00) « Avis 2/2000 concernant le reexamen général du cadre juridique dans le domaine des télécommunications » adopté le 3 février 2000, en particulier en ce qui concerne l'application des articles 6 et 7 de la directive 95/46/CE, WP 36 (5042/00) : « Avis 7/2000 sur la proposition, présentée par la Commission, de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 (COM (2000) 385) », adopté le 2 novembre 2000 et WP 37 (5063/00) : Document de travail « Le respect de la vie privée sur Internet — Une approche européenne intégrée de la protection des données en ligne », adopté le 21 novembre 2000.

à une telle utilisation directement lors de la collecte (case à cocher en ligne)[1]. L'envoi d'un courrier électronique à caractère promotionnel dans ces conditions doit également s'accompagner de la possibilité de retrait en ligne de la liste d'envoi utilisée[2].

29 — En ce qui concerne l'envoi de lettres d'information :

— Il convient de s'assurer de l'accord préalable de la personne concernée et du fait qu'elle puisse renoncer à l'abonnement de manière effective et à tout moment. Les personnes devront être informées de cette possibilité lors de l'envoi de chaque lettre d'information.

Le groupe de travail invite le Conseil, la Commission européenne, le Parlement européen et les États membres à tenir compte de la présente recommandation.

Le groupe de travail se réserve le droit de formuler d'autres observations.

Fait à Bruxelles, le 21 mai 2001.

Pour le groupe de travail

Stefano RODOTA

Président

[1] Au sein de l'Union européenne, cinq États membres (Allemagne, Autriche, Italie, Finlande et Danemark) ont adopté des mesures visant à interdire les communications commerciales non sollicitées. Dans les autres États membres, la situation n'est pas très claire ou il existe un système d'opposition. Il convient de noter que la proposition, présentée par la Commission, de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (COM (2000) 385) du 12 juillet 2000 préconise une solution harmonisée fondée sur l'approche du choix explicite qui a été approuvée à l'unanimité par le groupe de travail dans son avis 7/2000 (WP 36 cité ci-dessus). Voir également l'étude de S. Gauthronet et E. Drouard (ARETE) pour la Commission intitulée «Communications commerciales non sollicitées et protection des données», janvier 2001, hrrp://europa.eu.int/comm/inrernal_marke|/fr/media/dataprof/studies/spamsumfr.pdf

[2] Les exigences supplémentaires liées aux communications commerciales non sollicitées lorsqu'une opposition est possible au titre de la directive 97/66/CE sont définies dans la directive relative au commerce électronique.

Table des matières

Chapitre 3

Commission nationale de l'informatique et des libertés

21, rue Saint-Guillaume

75340 Paris Cedex 07

Tél. 01 53 73 22 22

Télécopie : 01 53 73 22 00

POUR PLUS D'INFORMATIONS:

Site Internet : http://www.cnil.fr

Imprimé en France par INSTAPRINT S.A.
1-2-3, levée de la Loire - LA RICHE - B.P. 5927 - 37059 TOURS Cedex 1
Tél. 02 47 38 16 04

Dépôt légal 2' trimestre 2002 / 06029984-2000

Le 22e rapport d'activité de la Commission Nationale de l'Informatique et des Libertés présente l'activité de la CNIL tout au long de l'année 2001 . Il constitue un ouvrage précis et complet pour tous les spécialistes des problématiques de la protection des données personnelles, mais également un moyen facile d'accès et passionnant pour le lecteur non-averti souhaitant appréhender ces questions avec curiosité.

En particulier, ce 22e rapport rassemble en une même partie, « Les débats en cours », tous les sujets actuellement débattus et qui certainement feront l'objet de décisions importantes dans un proche avenir. Tel est le cas du marché de l'identité numérique, de l'« e-administration », des listes noires ou bien du vaste domaine des applications de la biométrie.

Parmi les très nombreux dossiers reçus et instruits par la CNIL en 2001, une place particulière a été réservée à ceux, par l'importance des positions prises par la Commission, qui appellent un commentaire approfondi. Tel est le cas du traitement des données personnelles lors des fusions d'entreprises, des locataires de logements sociaux, de la cybersurveillance sur les lieux de travail, du système national d'information sur les dépenses de santé, de la diffusion de données personnelles sur Internet ou des droits particuliers des mineurs sur Internet.

Enfin, la dernière partie de ce rapport est consacrée à un panorama complet de la protection des données personnelles dans le monde, laissant une place importante aux travaux menés au sein de l'Union européenne.

Prix : 21 €
La Documentation française
29-3 1, quai Voltaire
75344 Paris Cedex 07
Téléphone : 01 40 15 70 00
Télécopie : 01 40 15 72 30
www.ladocumentationfrancaise.fr
Imprimé en France
ISBN : 2 1 1-005 16 3-9
DF : 5 6647-0