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

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'Économie, 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

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**	**5 617**	**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 œuvre 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'État, 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	**2**
— Fichier nat. informatisé de documentation de la Direction générale des douanes et droits indirect (FNID)	**1**
— Fichier TRACFIN (action contre les circuits financiers clandestins)	**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 GÉNÉRAUX

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 nominative 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'État, 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 Commission 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 président de la CNIL adresse ensuite au requérant une lettre lui indiquant qu'il a été procédé 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 les 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 MENÉES 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.

ÉVOLUTION 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 : — communication totale — communication partielle	93 65 % 75 18	65 60 % 27 38	59 70 % 44 15	74 69 % 63 11	82 59 % 75 7	90 80 % 84 6	82 84,5 % 79 3	86 83 % 85 1	**126** **78 %** **126** **—**	**757**

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 SYSTÈME 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 agricole, à propos de la constitution d'un système national interrégimes de l'assurance maladie (*cf. infra* chapitre 2, IV).

II. LES INTERVENTIONS LÉGISLATIVES

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 CRÉATION D'UN FICHIER NATIONAL AUTOMATISÉ 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'État 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 œuvre 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 ENQUÊTES 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 œuvre 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'État, 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 AUTOMATISÉ 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 OPÉRATEURS 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 malades : 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 œuvre 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 vœu 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'État 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 nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 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. 1113-6 nouveau du 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'État 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'État 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 vœu 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 dossier 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 Commission nationale de l'informatique et des libertés s'agissant des règles techniques 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 prospection 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 25 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 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 [1]. 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 *Le 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 (21e 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 États-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 HÉRITIERS SUR LES DONNÉES À CARACTÈRE PERSONNEL DE LEURS PARENTS DÉCÉDÉS

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 RÉGISSANT 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 1995, 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 œuvre. 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 PÉNALITÉS RÉPRIMANT 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 CONTRÔLE 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 œuvre 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.

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 CLIENTÈLE 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+ 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 œuvre 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 (nº 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'informa-

tion 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'effectivité de la mise en œuvre des mesures prises par Canal+ Distribution et Canal+ SA en application de la présente délibération.

II. DONNÉES 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.* 21e 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 œuvre 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 personnes concernées, ne saurait être collectée auprès des demandeurs de logement. Par ailleurs, aucune information relative aux « origines » du demandeur ou au pays de naissance de ses parents n'est pertinente au regard 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 élément d'état civil. La finalité des traitements de gestion des demandes de logements 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 départementaux d'action sociale, un critère devant être pris en compte pour apprécier l'ordre de priorité de l'examen de la demande. Si cette information est susceptible de déterminer des mesures particulières d'accompagnement social au bénéfice des personnes concernées, sa collecte systématique ne devrait 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 œuvre de procéder à des interrogations fréquentes sur la nationalité des intéressés. En tout état de cause, les textes législatifs et réglementaires régissant les enquêtes d'occupation des logements sociaux et les enquêtes de supplément de loyer solidarité ne mentionnent 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 considérée 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 doivent être pertinentes, adéquates et non excessives au regard de la finalité du traitement. Ces informations qui doivent être objectives et ne résulter d'aucun 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 III 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 peuvent 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.* 21e 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.

À 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 PROPORTIONNALITÉ

« 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 œuvre 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 SYSTÈME 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 SÉCURITÉ 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 œuvre 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 SANTÉ

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

La CNAMTS s'est ainsi engagée à 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. 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 catégories de professionnels responsables de ces dépenses et par professionnel 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 pertinentes 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 présente 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 bénéficiaires 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'« anonymisation » 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) c'est-à-dire au « transcodage » de ces matricules, selon un dispositif de codage irréversible, en des numéros non signifiants qui permettront 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 informations relatives à une même personne soient différents des numéros d'anonymisation créés par les caisses et utilisés lors de la transmission ;
— afin de prévenir tout risque de réidentification d'une personne par recoupement de plusieurs informations, seront interdites certaines recherches croisées à partir de variables potentiellement identifiantes (mois de naissance et 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) ;
— un logiciel de filtrage permettra de recenser toute requête dont le dénombrement des bénéficiaires concernés sera inférieur ou égal à dix, et d'interdire 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'Économie, 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 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) ;
— 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 œuvre 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 œuvre 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 DONNÉES 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 *Journal 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 soit 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 œuvre 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 œuvre 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 mœurs 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 nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret nº 78-774 du 17 juillet 1978 ;

Vu la délibération de la Commission nº 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'État, 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-Dumas, 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'État, 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 œuvre 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 œuvre 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 décisions prononcées par les juridictions constituent, si elles comportent le nom des parties, des traitements automatisés de données nominatives ; elles doivent, 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 constitution, sous une forme nominative, de telles bases de données par les juridictions 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'Église 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.familysearch.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 1960 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 États-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 dispositions 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 généalogique 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 microfilms et que cette même interdiction pèse sur les tiers à qui la société pourrait 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 nécessaire, au regard des dispositions de la loi du 6 janvier 1978, de soumettre 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 nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret nº 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 nº 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 *1978 ;*

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 nº 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 nº 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 surfant 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 œuvre, sur l'initiative de la CNIL, avec le concours du ministère de l'Éducation 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.

LES DÉBATS 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 MARCHÉ DE L'IDENTITÉ NUMÉRIQUE

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 œuvre 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 États*

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 cœur des politiques de réforme de l'État 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 États 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 ÉLECTRONIQUE 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 œuvre 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 PRÉALABLE : 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 lorsqu'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 le 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 Nationale).

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 IDÉES À 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 avatages 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 RÉFLEXION RENOUVELÉE 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'OÙ 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 SÉCURITÉ 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 œuvre 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 ÊTRE LE DEGRÉ 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, à 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 dispositifs 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'Économie, 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 PLACÉ AU CENTRE DU SYSTÈME 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.

À 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 CENTRALISÉE, DES ACCÈS DÉMULTIPLIÉS

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 OPÉRATIONS 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 PREMIÈRES ÉTAPES 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 œuvre 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 quater 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'Économie, 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 (DGI), 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.

« TéléTVA » 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 électronique 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 régime 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 délimiter 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 déclaration 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 permettre le transfert des fichiers d'ordinateur à ordinateur. Le déclarant est invité 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'administration, 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 personnel.

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 navigateur 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 sauvegarder 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 œuvre 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 œuvre 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 (CEDP) et un accusé de réception de paiement accompagné d'un numéro CPOP (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-TéléTVA », 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 transmission 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 œuvre 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 la 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'État 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 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 » ;
— 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 recours à la procédure de « rejeu » à l'existence d'un contentieux soient aménagées 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 délimiter 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 résultat 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 Commission souhaite qu'il intervienne dans les meilleurs délais, les contribuables adhérents 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 chiffrement 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 réduire le risque de mises en demeure intempestives en cas de dysfonctionnement 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'impôt 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'Économie, 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 (CDI) 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'authentification 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 la 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 impôts du traitement automatisé dénommé « Accès au dossier fiscal des particuliers ADONIS » ;
— de quatre projets d'arrêtés modificatifs modifiant respectivement les arrêtés du 25 juillet 1988 relatif à l'informatisation des inspections d'assiette et de documentation (traitement « ILIAD »), du 5 janvier 1990 relatif au traitement 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'ensemble 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 références 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 versements déclarés au titre des charges ;

— les données littérales ajoutées sur la déclaration électronique en contrepartie de la suppression de certaines pièces justificatives : nom des organismes bénéficiaires de dons, legs ou cotisations ouvrant droit à réduction d'impôt — à l'exception de ceux des organisations syndicales, des associations 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 projet 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'administration d'atteindre l'objectif voulu par le législateur — et que tout traitement 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 déclarations, 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'administration ;
— les avis d'imposition concernant l'impôt sur le revenu, les contributions sociales (CSG, CRDS), la taxe d'habitation et les taxes foncières ;
— une présentation synthétique du dossier fiscal du contribuable et un résumé 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 œuvre 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 [1] : 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. 20e 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 nº 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 nº 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 nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret nº 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 nº 99-1047 du 14 décembre 1999 pris pour l'application de l'article 107 de la loi de finances pour 1999 (nº 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 nº 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 Ier 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-I 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 œuvre 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 régime 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 contribuables 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 correspondantes 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-I 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'assurance 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 relevant 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.

La constitution des fichiers de restitutions

Selon l'article R.* 152-III 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 nº 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/ nº 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 /nº 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 œuvre 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 légitime 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 œuvre 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 Preventel 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'homonymie.

Compte tenu des nombreuses plaintes émanant de particuliers relatives à l'existence ou à la tenue du fichier Préventel, 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 la 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 œuvre 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 œuvre 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 œuvre 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 SIÈCLE DE BIOMÉTRIE

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^{78} 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 CARACTÉRISTIQUES COMMUNES DES SYSTÈMES 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 œuvre 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 œuvre 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 BioTrust 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 œil, 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°, 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'œil. 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 œuvre 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 DONNÉES 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 œuvre 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, tout 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 AUTORITÉS EUROPÉENNES 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 œuvre 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.

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 États 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 États-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[e] 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. 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 — COOPÉRATION 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 — SÉCURITÉ, 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 œuvre 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 œuvre 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 œuvre 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 États-Unis (*cf.* décision du 28 septembre 2001). Partageant l'avis selon lequel seule la conclusion d'un accord entre Europol et les États-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 États 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 CONFÉRENCE INTERNATIONALE DES COMMISSAIRES À LA 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, Égypte, 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 États 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.